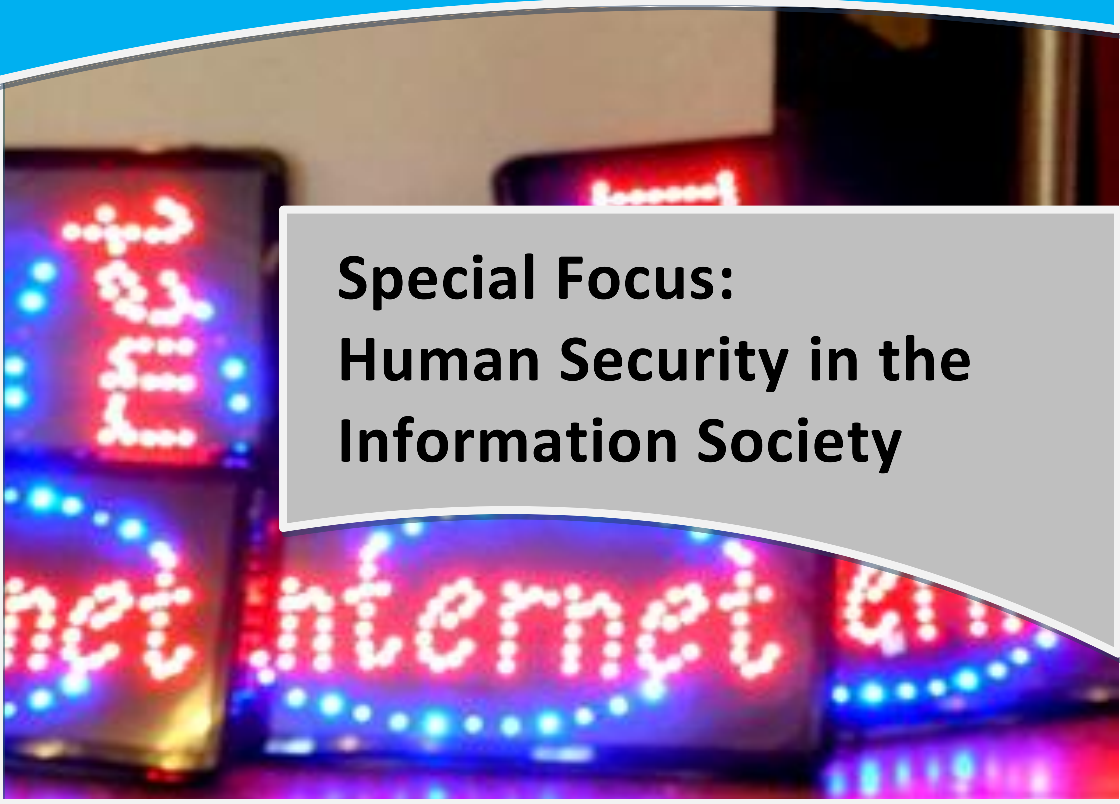
1
2012

Human Security Perspectives



Special Focus: Human Security in the Information Society

This edition of *Human Security Perspectives* has been edited by

Wolfgang Benedek
Matthias C. Kettemann
Heike Montag
Cristina Pace
Pascoal Santos Pereira

on behalf of the Human Security Focus Group at the Institute of International Law and International Relations of the University of Graz, Austria, and the European Training and Research Centre for Human Rights and Democracy (ETC), Graz.

This edition contains selected excellent contributions from the 5th Graz Workshop on the Future of Security on Human Security in the Information Society of 16 March 2012.

Articles

UNIVERSITY OF GRAZ
EUROPEAN TRAINING & RESEARCH CENTER
FOR HUMAN RIGHTS AND DEMOCRACY
ETC
UNI GRAZ

Human Rights @ Uni Graz
Learn all about our research, events and experts at uni-graz.at/humanrights

HUMAN SECURITY
FOCUS GROUP

European Training and Research Centre for Human Rights and Democracy
ETC GRAZ

Human Security Perspectives
Volume 9 (2012), Issue 1

Offenlegung gem. §25 österreichischem Mediengesetz/Impressum:

Herausgeber der Human Security Perspectives: Markus Möstl und Matthias C. Kettemann, für das Europäische Trainings- und Forschungszentrum für Menschenrechte und Demokratie (ETC)

Eigentümer und Verleger (100%):
Europäisches Trainings- und Forschungszentrum für Menschenrechte und Demokratie (ETC)

Herausgeber dieser Sondernummer:
Wolfgang Benedek, Matthias C. Kettemann, Heike Montag, Cristina Pace, Pascoal Santos Pereira für die Human Security Focus Group des Instituts für Völkerrecht und Internationale Beziehungen der Karl-Franzens-Universität Graz und des Europäischen Trainings- und Forschungszentrum für Menschenrechte und Demokratie (ETC)

Sitz/Redaktion:
Elisabethstrasse 50b, A-8010 Graz
Tel.: +43/(0)316/380 1535, Fax +43/(0)316/380 9797
E-Mail: humansecurity@uni-graz.at; matthias.kettemann@uni-graz.at; markus.moestl@uni-graz.at
Website: http://www.hs-perspectives.etc-graz.at

Unternehmer:
Unabhängiger, eingetragener Forschungsverein; dessen Vorstand vertreten durch Renate Kicker (Obfrau)

Offenlegung der Blattlinie gem. § 25 Abs. 4 Mediengesetz:
Human Security Perspectives ist eine unabhängige und überparteiliche elektronische Zeitschrift des Europäischen Trainings- und Forschungszentrums für Menschenrechte und Demokratie (ETC) und versteht sich als Informations- und Diskussionsplattform zu außen- und weltpolitischen Themen mit dem Schwerpunkt der Menschlichen Sicherheit (Human Security). Der Inhalt stellt die Meinung der jeweiligen Autoren dar.

Titeldesign:
Matthias C. Kettemann
(unter Verwendung eines Bildes © CC hdzimmermann, FlickR)

Table of Contents

III The Impact of ICTs on Human Rights Protection Regimes

IV Recent Developments

Wolfgang Benedek, Matthias C. Kettemann, Heike Montag, Cristina Pace, Pascoal Santos Pereira

Editors' Preface

The workshop organizing committee: Professor Wolfgang Benedek, Cristina Pace, Pascoal Santos Pereira, Heike Montag, Reinmar Nindler, Paul Gragl, Matthias C. Kettemann (from left to right). © University of Graz (2012)

Human Security in the Information Society

It was the fifth of its kind, but it was also unique, and uniquely timely: the 5th Graz Workshop on the Future of Security dedicated to *Human Security in the Information Society: Regulating Risks – Empowering People*.

Started in 2008, the Graz Workshops on the Future of Security have been successful in identifying some of the most burning issues of the international legal debate on the future of security and framing the debate.

With that in mind the organizers chose the role of human security in the information society as the topic of the 5th Graz Workshop. Organized by the Institute of International Law and International Relations of the University of Graz, together with the European Training and Research Centre for Human Rights and Democracy (ETC), and their Human Security Focus Group the workshop was held in cooperation with the Austrian National Defence Academy, the Austrian Institute for International Affairs (OIIP) and the Marie Curie Action “Sustainable Peace Building” funded under the EU’s 7th Framework Programme.

This challenging topic of human security in the information society united two of the central areas of research of the Institute of International Law and International Relations and the ETC: protecting human security and ensuring an effective and legitimate, human rights-sensitive Internet Governance.

Just as the four previous workshops, the 5th Graz Workshop on the Future of Security (16 March 2012) was dedicated to furthering the understanding of today’s and tomorrow’s security challenges and identifying practical answers. The organizers brought together promising pre- and postdoctoral researchers, as well as experts and practitioners from different countries and backgrounds who presented their latest research on issues ranging from Internet Governance to cybersecurity.

Human security is essential for a holistic, equitable and sustainable development of information society. Indeed, security has become a major issue for the information society as could be seen from the recent Munich Security Conference 2012 which had a focus on cybersecurity. The police is concerned with cybercrime, the military with cyberwar and the state with cybersecurity.

While the Cybercrime Convention of the Council of Europe of 2001 has addressed this issue relatively early, the problem of cyberwar has become an area of concern only recently.

The workshop itself encompassed two keynote sessions and two thematic sessions followed by a final high-level discussion focusing on different dimensions of human security in the information society. Selected contributions to these sections have now been revised and enlarged in order to be published. You can find them on the following pages of this edition of *Human Security Perspectives*, presented in four overarching sections.

Our first section brings together selected keynote addresses of the workshop. Wolfgang Benedek introduced the concept of information society in the context of human security. Furthermore, two speeches from practitioners' views were delivered. One by Jörg Leichtfried (MEP) on how the European Parliament safeguards human rights on the Internet and another by Gerhard Jandl from the Austrian Foreign Affairs Ministry on the challenges of cybersecurity from a governmental perspective.

The subsequent three sections of the current edition of *Human Security Perspectives* include selected excellent workshop papers and a concluding contribution on recent challenges of ensuring human rights online.

A first section focused on "Balancing Law, Technology and Human Rights" includes a paper by Farhan Sahito and Wolfgang Slany on functional Magnetic Resonance Imaging (fMRI) and how this technology can be a challenge to the balance between human security and state security. Cristina Pace enquired into the challenges of protecting both human rights and human security in the information society, with a focus on the protection of public security.

The following section addresses the "Impacts of ICTs on Human Rights Protection Regimes" in different contexts. Mahlet Fitsum Halefom provides a broad overview of the impact of social media and ICTs on conflict management and peace building. Maria Eduarda Gonçalves and Inês Andrade Jesus focus on security and personal data protection in the European Union.

In a final section dedicated to recent developments, Matthias C. Kettemann dissects the recent UN Human Rights Council Resolution on human rights on the Internet and sheds light on its content, potential, and relationship to human security.

Concluding, we would like to note with gratitude the contributions by the National Defence Academy of the Federal Ministry of Defence and Sports and the Federal Ministry of European and International Affairs of the Republic of Austria and by the Austrian Institute for International Affairs. Their representatives added an essential practical dimension to an academic exchange that succeeded in connecting emerging and established researcher on the pre- and postdoctoral level, active in the field of peace and conflict studies.

Graz, July 2012

Wolfgang Benedek, Matthias C. Kettemann,
Heike Montag, Cristina Pace, Pascoal Santos Pereira

I Keynotes

Wolfgang Benedek

Human Security in the Information Society

A Introduction

Security has also become a major issue for the information society as could be seen from the recent Munich Security Conference 2012 which had a focus on cybersecurity.[1] The police is concerned with cybercrime, the military with cyberwar and the state with cybersecurity in general, because cyberspace is increasingly being used

[1] See Weidlich, Anke and Petra Beenken, *MSC Booklet Paper: Cybersecurity*, Munich Security Conference, 2012, at: www.securityconference.de (All websites used in this essay were last checked on 29 July 2012).

in a way which threatens security in general and human security in particular. While the Cybercrime Convention of the Council of Europe of 2001 has addressed this issue relatively early, the problem of cyberwar has become an area of concern only recently. Broad attention was given to successful attempts to damage Iranian atomic infrastructure by electronic means, by the virus “Stuxnet” sent from somewhere without revealing the source of the attack.[2]

The issue of cyberwar and how humanitarian law can deal with it has been the topic of a recent doctoral thesis at the Institute of International Law and International Relations.[3] There has been a long standing focus on human security as well as on the information society in separate research programmes which are brought together for the first time in the workshop (at which the contributions of this journal were first presented) under the title of “Human Security and the Information Society”. However, while in the past the focus at the institute as well as at the European Training and Research Center for Human Rights and Democracy (ETC) has been on governance and human rights issues related to both human security and the information society[4], the inquiry into the relationship between the two concepts shows certain parallels: human security is concerned with the security of the human person rather than state security. The democratic state should have this focus in its security strategy anyway. Threats from the misuse of cyberspace do also affect the human person, whether in the form of spam, viruses or in the form of cyberattacks on vital critical infrastructures on which our computer systems and with

[2] See www.stuxnet.net.

[3] See Georg Kerschischnig, *Cyberthreats and International Law*, Utrecht, 2012.

[4] See the respective websites at www.uni-graz.at/vrewww/english/research/research/html and www.etc-graz.at.

them the whole society depends. Threats may also emanate from an illicit collection of data in social networks or search engines, which use this data mining to develop profiles of the users for commercial purposes which raises issues of privacy. In a similar way security services are gaining increasing access to data of internet users for their own purposes.

B The Meaning of Human Security in the Context of the Information Society

Dealing with security threats affecting the individual, the ordinary person, directly or indirectly, is the challenge of human security in the information society. These threats can relate to the freedom from fear, meaning personal security and threats to internet users, violating their civil and political rights or the freedom from want, meaning threats to internet users affecting their economic, social and cultural rights, the rights to education, to health or to development. The concept of human security also deals with the empowerment of the human person to deal with those threats.[5] Indeed, the internet provides opportunities of empowerment as can be seen from the Arab Spring or from various civil society initiatives like Avaaz campaigning globally for human concerns.[6] However, the

[5] See Oberleitner, Gerd, *Human Security*, in: Forsythe, David P. (ed.), *Encyclopedia Of Human Rights* (Volume 2), OUP, Oxford, 2009, pp. 486-493; UN Secretary-General, *Human Security, Report By The Secretary-General*, A/64/701, 8 March 2010; Benedek, Wolfgang, *Mainstreaming Human Security In Peace Operations And Crises Management – Policies And Practice*, in: Benedek, Wolfgang, Matthias C. Kettemann and Markus Möstl (eds.), *Mainstreaming Human Security In Peace Operations And Crises Management – Policies, Problems, Potential*, Routledge, London, 2010, pp. 13-31.

[6] See www.avaaz.org.

same internet can also be misused by governments to establish a stronger control over the individual and, for example, limit its freedom of expression.

One particularity of human security in the information society is that the internet allows for a decentralized and participatory approach to issues of concern and in this way for democratic responses to security challenges in comparison to more centralized and authoritarian or top down responses in the security sector in general. The user and their needs should be central and indeed the user perspective is given much attention in the information society.[7] This more participatory approach can be seen also in the principle of the multi-stakeholder partnership (MSP) according to which all actors are to be included in internet governance, which is at the basis of internet democracy.[8] Rule of law and good governance should also be features of both human security and internet governance, which should be participatory and not exclusive.

While the traditional perspective on security risks is to care about the security of the state, a focus on human security reminds the state that in the end it is the security of its people, on which its existence is founded. However, the internet has brought with it new vulnerabilities, so called “cyberthreats”, which consist in various forms of cyberintrusions, which range from cyberattacks like Denial of Service (DoS) attacks, viruses, worms, trojans or botnets, threatening critical infrastructures, to the activities of so-called “cybervigilantes”, hackers which use their knowledge for what they perceive as public concerns,

[7] The Council of Europe, for instance, is in the process of elaborating a compendium of user rights.

[8] See World Summit for the Information Society (WSIS), *Geneva Declaration of Principles*, WSIS-03/GENEVA/A/DOC/4-E, 2003, at para. 49 and *Tunis Commitment*, WSIS-05/TUNIS/DOC/7-E, 2005, at paras. 34 and 35.

while cybercriminals pursue their own agenda. The issue of resilience of critical infrastructures against such attacks has become the major challenge today.[9]

There have already been several attacks against the stability of the internet, including those in 2007 against Estonia, or in 2008 against Georgia during the conflict about South Ossetia or more recently in the Arab-Israeli conflict. Some will also remember the attacks which Google reported to have experienced from the Chinese side and which led Google to partly withdraw its business from China. There has been criticism of certain companies like Yahoo that they have collaborated with the Chinese government leading to the arrest of human rights defenders, which means that human security can also be and often is threatened from the side of private internet companies, raising the issue of responsibility of internet intermediaries to their users.[10]

The security of the individual can be threatened in many more ways, in particular with regard to its privacy or the security of its data as can been seen from the discussion about the Data Retention Directive of the European Union, about Google Street View, about cloud computing or about of the Internet of Things, which, by attaching tiny tags on clothes could (if these tags communicate) result in a nearly total control of the citizen. Accordingly, there is a growing relevance of the law of data protection based on the human right to privacy. In this context, human rights are linked with human security

[9] See Vilnius IGF Meeting, Background Paper, *Legal Aspects of Internet Governance: International Cooperation On Cyber-security*, 2010. Available online at: http://meetings.abanet.org/webupload/commupload/CL320061/relatedresources/IGF_Vilnius_Workshop_123_Background_Paper_Final.pdf.

[10] See Schellekens, Maurice, *Liability Of Internet Intermediaries: A Slippery Slope?*, SCRIPTed (Volume 8, Issue 2), 2011, pp. 154-174.

because human rights also protect and empower the individual. Whereas human security requires a political commitment, which is not always translated into law, human rights must be respected by states and often also non-state actors as binding law.[11]

More threats against the individual in the context of the information society are related to digital identity theft, to hate speech, child pornography, racism or extremism on the internet, which shows that in the information society the individual is faced with some specific vulnerabilities, which need to be addressed by concepts of human security. The individual may also become victim of counter measures taken for its protection like in the case of the Danish police blocking Google and Facebook in an effort to block illicit websites.

A particularly vulnerable group is the group of children, which are faced with specific threats like grooming, exposure, sexting[12] or child pornography, which requires measures of specific protection as indicated in the recent “User Strategy for a Safer Internet for Children and Teenagers” of the European Union.[13] There, measures are foreseen for a high-quality online content for children and young people, for stepping up awareness and empowerment, for creating a safe environment for children

[11] See Benedek, Wolfgang, *Human Security And Human Rights Interaction*, in: Moufida Goucha and John Crowley (eds.), Rethinking Human Security, International Social Science Journal (Volume 59, Supplement 1), 2008, pp. 7-18.

[12] Cf. Kettemann, Matthias C., *Taking Sexting Seriously: Should Europe Start Prosecuting "Sexters"*, juridikum (Volume 4), 2010, pp. 402-413.

[13] See European Commission, *Digital Agenda: New Strategy For Safer Internet And Better Internet Content For Children And Teenagers*, IP/12/445, 2012. Available online at: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/445&format=HTML&aged=0&language=EN&guiLanguage=en.

online and for fighting against child sexual abuse and exploitation.

These threats obviously are not coming from states, but rather from other individuals, hackers, people inciting to violence, glorifying terrorism or recruiting for it, using hate speech or propagating racism and xenophobia. There are different approaches how to deal with these threats. According to human rights law the state has an obligation to protect the individual against certain of these threats and it can make use of the limitations of the freedom of expression to do so. However, the continental European approach and the Anglo-American approach, in particular the approach of the United States based on the freedom of speech in the Second Amendment to the US constitution are quite different, which is also reflected in the fact that the United States has not signed the additional protocol to the cybercrime convention on hate speech.[14]

This shows that more than in other security contexts the individual is personally affected by threats to human security in the information society. Also, the individual or non-state-actors are more involved than in other security contexts, both as perpetrators and as victims or targets of attacks. Borders obviously do not play much of a role any more. When it comes to threats or attacks, whereas they are still quite relevant when it comes to acting against such attacks as can be seen from the difficulties of jurisdiction and prosecution in the context of the cybercrime convention. Further issues emanate from the fact that some of the illegal measures might have been taken in the public interest, like in the case of

[14] Von Blarcum, Christopher D., *Internet Hate Speech: The European Framework And The Emerging American Haven*, Washington & Lee Law Review (Volume 62), 2005, pp. 781-830.

"Anonymous" or "Wikileaks", although this might be seen differently by the states affected.

Particular problems arise from situations, when the state is the author or source of the insecurity, by blocking, filtering or even blacking out the internet,[15] by retaining and analyzing personal data or by requiring intermediaries like internet service providers to do so. There is a major debate on to what extent the state should get involved in sanctioning or preventing copyright violations. "Three-strike-laws" or other sanctions which disconnect users from the internet can never be justified by copyright violations as also Viviane Reding, the European Commissioner for Justice and Fundamental Rights confirms.[16] However, there has been even a case of extradition of a student from the UK to the United States for similar offences.[17] There is also the danger of applying anti-terrorism laws or laws against organized crime against hackers like in the case of "Anonymous", which all raise issues regarding the application of the principle of proportionality, which in the end can only be resolved by a competent court, because each government might draw the line differently.

Accordingly, there is a need for protection against security risks, but it is not only the state which has a

[15] Cf. on the legality of blackouts, Kettemann, Matthias C., *Nationale Sicherheit und Informationsfreiheit* [National Security and Freedom of Information], in: Schmalenbach, Kirsten (ed.), *Tagungsband Österreichischer Völkerrechtstag 2011* [Collected Contributions to the 36th Annual Austrian Conference on International Law 2011], Vienna, 2012 [in print].

[16] Statement by Reding, Viviane, Vice-President of the European Commission and EU Commissioner on Justice, Fundamental Rights and Citizenship. Available online at: http://ec.europa.eu/commission_2010-2014/reding/pdf/quote_statement_en.pdf.

[17] BBC, *Richard O'Dwyer case: TVShack creator's US extradition approved*, 13 March 2012. Available online at: http://www.bbc.co.uk/news/uk-england-south-yorkshire-17355203.

responsibility in this context but also the individual user, whether he or she uses a firewall, participates in international alerts or resorts to existing hotlines, where misuse of the internet can be reported. Again the question needs to be addressed what happens with such reports and whether they are dealt with in a professional way. But it corresponds to the decentralized nature of the internet that users also develop a particular responsibility for protecting cyberspace as a common public good and do not leave this task to states or companies alone.

C Measures of Protection of Human Security in the Information Society

Human security in the information society is also characterized by the specificities of the multi-stakeholder approach. Accordingly, all actors can be subject to threats, but also be involved in remedial measures. The rules applying to the internet are characterized by the principle that what applies offline should also be respected online. Guidance is provided by various efforts to redefine and interpret human rights for the needs of the internet and by drawing up catalogues of principles for human rights in the internet or for internet governance. The human security concept is characterized by the respect for human rights which is also relevant for security threats related to the internet. One effort in this context is the Charter on Human Rights and Principles for the Internet,[18] which is based on the Universal Declaration on Human Rights and tries to provide a comprehensive approach to the interpretation of human rights for the information society. A short version can be found in the “Ten Rights and Principles for the

[18] For the Charter on Internet Rights and Principles of the Internet and the ten key rights and principles, see http://irpcharter.org.

Internet" elaborated as in the case of the Charter by the Dynamic Coalition on Internet Rights and Principles. Also the Special Rapporteur on Freedom of Expression in his report of 2011 put particular emphasis on the threats to freedom of expression in the context of the information society. He identified certain practices of authoritarian states to block or to filter the internet and to turn it into an instrument of control of their citizens. At the same time he highlighted the opportunities related to the internet for the fuller realization of human rights as in the case of the freedom of expression and democracy, as can be seen from the Arab spring.[19]

The Council of Europe has taken a leading role in developing guidelines, codes of conduct and recommendations on preserving the protection of the public service value of the internet, in particular also in the context of human rights in the internet.[20] Business is another important actor and there are a number of good practices like the Global Network Initiative undertaken by Google, Twitter, Yahoo and Microsoft as well as others in order to provide more transparency and to uphold freedom of expression and the right to privacy. An example in case is the transparency report issued by Google[21] or the Webpage "chilling effects" by the Electronic Frontier Foundation and major US universities.[22]

[19] La Rue, Frank, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, A/HRC/17/27 of 26 April 2011.

[20] Kettemann, Matthias C., *Ensuring Human Rights Online: An Appraisal of Selected Council of Europe Initiatives in the Information Society Sector in 2010*, in: Benedek, Wolfgang, Florence Benoit-Rohmer, Wolfram Karl and Manfred Nowak (eds.), *European Yearbook On Human Rights*, Intersentia, Vienna, 2011, pp. 248-267.

[21] Google Transparency Report. Available online at: http://www.google.com/transparencyreport.

[22] See www.chillingeffects.org.

The role of technology and of business, of companies active in the internet deserve special attention as they can be both perpetrators and victims of measures violating human security. For example, the issue of complicity with authoritarian governments by making their technology available has only recently been discussed in the case of the European Parliament, but there are many more such cases.[23] Companies like Google which follow the principle of "do no evil" have already reacted to some of the challenges to human security of their users. However, they are also under attack for the commercial use they make of the data of their users often without obtaining their consent. A recent call on companies not to make their technology available to Pakistan to install a new server system to blog access to certain websites shows the role of civil society in upholding the openness of the internet. However, efforts by governments to control the internet are not limited to China or authoritarian states in the South, they exist as well in the United States and other Western countries as the international appeals of civil society against recent legal projects strengthening the control and establishing new monitoring systems for the internet for security purposes have shown.[24]

The need for more cooperation is undisputed, but the proposal for a (UN) global cyber treaty or efforts to establish with the help of the International Telecommunication Union (ITU), which is a UN specialized agency, a stronger control of states over the internet have alarmed the internet community in general, and civil society in particular.

The self organisation by the community of internet users to protect cyberspace against misuse can also be

[23] Cf. the contribution by Jörg Leichtfried, in this journal.

[24] Cf. CNN (Dan Mitchell), *How Social Media Killed ACTA*, 6 July 2012, available online at: http://tech.fortune.cnn.com/2012/07/06/how-social-media-killed-acta.

problematic, if self-appointed watch dogs, so-called “cybercops” denounce what they consider as illicit speech. However, there are also others to correct them as it can be seen in the system of Wikipedia. Accordingly, there is a need for a permanent dialogue between all actors of the internet community as it is indeed happening in the yearly Internet Governance Forum since 2006. The fact that legal boundaries do not play the same role in the information society requires a stronger cooperation of all actors and a constant effort to develop a consensus on common rules and principles.

The forthcoming general conference of ITU will show how far efforts in the direction of a top-down approach by states will find supporters. With the growing relevance of the internet in the field of security one cannot be surprised that states try to gain more control about internet governance, where from the beginning the driving forces were technology and business as well as civil society. However, there are hardly any multi-stakeholder approaches, when it comes to security in the internet, which shows that the principle of the World Summit on the Information Society according to which internet governance is to follow the multi-stakeholder approach has to be re-confirmed constantly, in particular against challenges from certain states.

D How to Respond to Challenges to Human Security in the Information Society?

The human security approach requires that security is protected in a way which respects human rights. Human rights are international obligations, which can only be restricted under certain conditions, which have to follow a three-part test of being based on law, being necessary in a democratic society and proportional to the objective to be achieved.

Security measures which do not respect human rights do not increase the security of the people. Emergency measures have to follow the rules for emergencies as indicated in international human rights law. The Council of Europe has developed certain codes of conduct and guidelines to maintain human rights obligations when taking restrictive measures.[25] Civil society consisting of various NGOs active in the field of the information society has established itself as a watch dog for action against restrictive measures and for the protection of human rights.

E Conclusion and Outlook

According to the concept of human security, the state has the obligation to protect its citizens, but also to empower them to protect themselves. In the ideal way state security should be equal to human security. As restrictive measures against an open internet by states have shown, certain authoritarian states restrict the internet in order to protect themselves against their citizens or civil society worldwide as could be seen in the case of the Arab Spring with the Egyptian blackout or the efforts of Syria and others to use the internet to control dissidents. Fortunately, there is also circumvention technology available, which is offered by certain NGOs, sometimes with the support of human rights-minded states or the EU. Freedom of expression on the internet has gained a new significance and goes far beyond what in the past used to

[25] See Council of Europe, *Guidelines On Human Rights And The Fight Against Terrorism*, 11 July 2002. Available online at: http://www1.umn.edu/humanrts/instree/HR%20and%20the%20fight%20against%20terrorism.pdf.

be free speech or free media. No doubt a certain responsibility from the side of the users is also necessary in order to avoid misusing the internet for hate speech or extremism of all kind which may incite to violence.

The internet is a good example for the challenges of state security versus human security, namely whether the internet is used to control people or to empower people. Certainly there has always to be some balancing of interests, but for this purpose the legitimate restrictions of human rights show the way.

Accordingly, the principles of internet governance have to take principles of human security into account as they do with regard to the obligations of human rights. The multi-stakeholder approach is crucial to develop cooperative attitudes, starting from a permanent dialogue among all actors. If these principles are not respected all actors should cooperate to prevent abuse and to defend the rights of all internet users.

Jörg Leichtfried

How the European Parliament Safeguards Human Rights on the Internet

© Nindler 2012

A No Disconnect Strategy

Social networks, mobile devices and the Internet nowadays play a central role in democratic movements. This was shown by the protests in Iran and the Arab Spring. Hillary Clinton described such technologies as "freedom technologies".

The spread of these new communication tools leads to an increase of surveillance technologies in many States. The EU has appointed a former German Defense

Minister to advice on how to provide ongoing support to Internet users, bloggers and cyber-activists living under authoritarian regimes, as part of its ‘No Disconnect Strategy’, launched in Brussels to protect Internet access as a driver of political freedom.

Announcing the Strategy, the Vice-President of the European Commission responsible for the Digital Agenda, Neelie Kroes, told a press conference that the Arab Spring was a wake-up call. She said that in Egypt, social media allowed people to bypass state-run media, and pointed out that in 1982 in Syria, the Hama massacre was hidden for months: “In 2011 video-sharing services helped expose regime abuses. They made us aware of this and being better taking action.” “Repressive regimes now understand the power of these networks and have tried to turn them off,” she added. “They did not succeed. And the EU is working to ensure online rights are respected like offline rights.”

Expressing her support for the initiative, EU High Representative for Foreign Affairs Catherine Ashton said: “The right to communicate freely is a key part of basic human rights. The Internet and social media have become an important way of promoting freedom of expression. That's why the EU is determined to resist any unjustified restrictions on the Internet and other new media.”

Kroes said she had invited Karl-Theodor zu Guttenberg, a former Federal Minister of Defense, and of Economics and Technology, in Germany, to assist her on the issue. This appointment is a key element of the new ‘No Disconnect Strategy’ to uphold the EU's commitment to ensuring human rights and fundamental freedoms both online and offline, and that Internet and other information and communication technologies (ICTs) can remain a driver of political freedom, democratic development and economic growth. Karl-Theodor zu Guttenberg will liaise with member states, third countries and NGOs which are committed to working in this area and advice on how to advance the strategy in a coordinated and effective manner. Kroes said his experience would be crucial: “As a former head of armed and security services, with deep experience in foreign affairs, I know Karl-Theodor can have the right conversations and give Internet freedom the prominence it deserves.”

The ‘No Disconnect Strategy’ will assist citizens in four ways:

- Developing and providing technological tools to enhance privacy and security of people living in non-democratic regimes when using ICT.
- Educating and raising awareness of activists about the opportunities and risks of ICT. In particular assisting activists to make best use of tools such as social networks and blogs while raising awareness of surveillance risks when communicating via ICT.
- Gathering high quality intelligence about what is happening on the ground in order to monitor the level of surveillance and censorship at a given time, in a given place.
- Developing a practical way to ensure that all stakeholders can share information on their activity and promote multilateral action and building cross-regional cooperation to protect human rights.

Vice-President Kroes said she could not speak publicly about all the elements of the strategy, but highlighted three of its most important actions:

- Deployment of "Internet survival packs" to activists. These are easy-to-use software/hardware packages helping people to bypass censorship and counter surveillance.

- Stimulating EU companies to develop self-regulatory approaches (or join existing ones, such as the Global Network Initiative) so they stop selling despots their ICT tools of repression.
- Hosting support – to help prohibited content reach its audience (blogs and videos for example) and to allow anonymous usage of the internet.

The Joint Communication, "A Partnership for Democracy and Shared Prosperity with the Southern Mediterranean" committed the European Commission to develop tools to allow the EU, in appropriate cases, to assist civil society organizations or individual citizens to circumvent arbitrary disruptions to access to electronic communications technologies, including the internet. This followed evidence of such disruption or attempted disruption by authoritarian governments during the Arab Spring uprising, for example in Egypt.

B ACTA

The Socialists and Democrats (S&D) Group fully acknowledges the many serious concerns that EU citizens and civil society have expressed about the Anti-Counterfeiting Trade Agreement (ACTA).

There is no doubt that violations of intellectual property rights (IPR) are increasing and that counterfeiting of goods and brands must be tackled at international level. While European consumers rely on EU legislation to protect them from the risk of fake products ranging from car parts to children's toys and medicines, we question whether ACTA is the right tool to fight against counterfeiting at the international level, particularly as several large countries are not signatories to the agreement.

Our main criticism centers on copyright enforcement on the Internet and the definition and monitoring of activities online. The text of ACTA is too vague and we need to have clarification of the role of Internet service providers (ISPs) in policing the agreement. The enforcement of intellectual property rights cannot come at the expense of curtailing civil liberties and data protection especially when it comes to online activities. We also regret the fact that copyright infringements online are treated in the same manner as counterfeiting of goods and brand. We take the view that it is wrong to attempt to tackle both issues with the same instrument.

The European Parliament will not be rushed to give its consent on ACTA. We want to have a fact-based discussion with representatives of all sides, so that we can make a fully informed decision – securing the rights of citizens to the protection of personal data whilst benefiting from the production, exchange and distribution of culture and knowledge as well as the rights of copyright holders and other interest groups.

1 The ACTA Proposal

Firstly, the S&D Group regrets the way negotiations were carried out, as stated in our previous resolutions. We have always been at the forefront of demanding that information is made public. We also find it unacceptable that the European Parliament, as the directly elected institution of the EU was not given any say over the content of the agreement.

Some parts of ACTA could be beneficial and could help curtail the criminal trade in fake and counterfeited products. We do, however, have serious concerns about copyright enforcement online, especially the obligation to apply criminal sanctions without the necessary provision of binding safeguards for personal users, as well as the vague definition of terms, particularly referred to the concept of "commercial use".

We must avoid the risk that ISPs are given the task to control content, thus becoming Internet regulators. Law enforcement must not be privatized. This situation must be properly clarified. We were happy to see the so-called “three-strikes-rule" removed from ACTA so that people will not be arbitrarily prevented from having access to the internet.

All the same, the fear remains that providers could be obliged to block or prevent users having access to the internet, due to the vague definition of terms. Data protection must also be ensured at the highest level, especially in international data exchange that is foreseen by the agreement. ACTA must absolutely not prevent the legitimate production and access to generic medicines, much of which is destined for the developing world. We will seek to clarify the legality of ACTA and make sure it falls within existing EU law, including full compliance with the EU Charter of Fundamental rights.

Moreover, we have concerns that ACTA has reduced the possibility for the European Parliament to modify EU IPR legislation. We believe EU should have first reviewed the IPR Enforcement Directive (IPRED) and adapted EU law towards the Internet environment before negotiating such an agreement.

2 How We Will Proceed?

On 12 April 2012 a discussion was organized with representatives from all sides of the debate, so that the parliamentarians can hear firsthand the opinions on ACTA. This will just be one part of the continuing dialogue we will have with all those concerned.

The Commission decided to refer ACTA to the ECJ. The S&D-group will not refer the ACTA-agreement to the

ECJ. We want assurances that ACTA will not lead to the infringement of free movement of goods and persons within EU, nor of other fundamental rights. Even if the ECJ gives a positive opinion on the matter, we will make our own independent decision on ACTA when it comes back to the EP.

The International Trade Committee wants to stick to the foreseen timetable. That means, that the voting in the International Trademark Association (INTA)-Committee should be take place in May, the voting in the plenary is foreseen for June, July or September. The Legal Affairs, the Industry, Research and Energy, and the Development committees will also publicly discuss the proposal in the coming months. The Civil Liberties Committee will publicly discuss and deliberate on the compatibility of ACTA with the Charter of Fundamental Rights, as already requested by the Parliament's Plenary and produce an extensive report of the findings.

It is essential that ACTA is now subject to full democratic scrutiny of the EP, although at this stage of the process, the Parliament can only say yes or no and has no possibility to amend the text. We will seek answers to all of our questions and concerns, through ongoing dialogue also with citizens, institutions and groups concerned. For the moment the S&D group would rather vote against the ACTA agreement.

C Contradictions between Protecting Human Rights and Exporting Surveillance Technologies

On the one hand the EC had no intent to limit the export of dual-use-goods before the new directive came out and on the other hand the EC intends to protect the human rights on the Internet and Internet freedom in general. This is a big contradiction. For example, a EU-based company exported the Software "Finisher" to Egypt and the Hosni

Mubarak regime. This software helped to the regime censor the Internet and to find out the names and identities of the blogger. German journalists from Central German Broadcasting (MDR) proved that with the help of "Finisher" a lot of anti-Mubarak activists were identified, arrested and some were also killed.

1 Controlling Dual-Use Exports

Parliament revised EU rules on exports of products that can be used for civilian and military purposes, such as chemicals, telecom devices or software. In negotiations with the Council, MEPs won an undertaking that no general export authorization should be given to dual-use technologies that can potentially be used in ways that violate human rights.

In the legislative resolution by Jörg Leichtfried adopted with 567 votes in favour, 89 against, and 12 abstentions, MEPs prohibit the granting of general EU authorizations for exports to certain countries (such as China, India, Russia and Turkey) of telecommunication technologies that can be used "in connection with a violation of human rights, democratic principles or freedom of speech (...) by using interception technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of Internet use". Today, exports of these products have not been subject to any EU authorization system, and it has been up to individual member states to decide on unilateral export controls.

In my opinion, this is a good step towards strengthened control over dual-use products exported from the EU, a bigger step could have been taken if we had established a system of pre-export notifications, but unfortunately there was no majority in the EP for such an amendment.

The Parliament also prohibited dual-use exports to countries under arms embargoes imposed by the EU Council, the OSCE or the UN. To strengthen parliamentary scrutiny over export authorization procedures, MEPs insisted that each year the Commission should present an annual report to the Parliament on dual-use exports. Exports of dual-use items are restricted by a system of international, EU and national rules, which require EU firms to seek authorization from the authorities. These rules aim to limit the risk of sensitive dual-use items being used for military purposes.

2 Reporters without Borders: For Freedom of Information

The last report, released in March 2011 at the climax of the Arab Spring, highlighted the fact that the Internet and social networks have been conclusively established as tools for protest, campaigning and circulating information, and as vehicles for freedom. In the months that followed, repressive regimes responded with tougher measures to what they regarded as unacceptable attempts to "destabilize" their authority.

In 2011, netizens (active participants in Internet world) were at the heart of the political changes in the Arab world and elsewhere. They tried to resist the imposition of a news and information blackout but paid a high price.

As the numbers of protesters grow, more and more of them are at risk. At least 199 cases of arrests of netizens were recorded in 2011, a 31 percent increase compared with the previous year. Today, at least 120 netizens are in prison because of their activities. China, followed by Vietnam and Iran, has the largest number of netizens in prison again this year.

3 Bahrain and Belarus, New Enemies of the Internet

Two countries, Bahrain and Belarus, have been moved from the “under surveillance” category to the “Enemies of the Internet” list, joining the ranks of the countries that restrict Internet freedom the most: Burma, China, Cuba, Iran, North Korea, Saudi Arabia, Syria, Turkmenistan, Uzbekistan and Vietnam. They combine often drastic content filtering with access restrictions, tracking of cyber-dissidents and online propaganda. Iran and China, in particular, reinforced their technical capacity in 2011 and China stepped up pressure on privately-owned Internet companies in order to secure their collaboration.

4 The Internet is Increasingly Important to Fight Dictatorial Systems

The protests in Egypt were organized to a large degree via the Internet and social media.

Khaled Saeed was a young Egyptian man who died under disputed circumstances on 6 June 2010, after being arrested by Egyptian police. Photos of his disfigured corpse spread throughout online communities and incited outrage over allegations that he was beaten to death by Egyptian security forces. A prominent Facebook group, "We are all Khaled Said", brought attention to his death and contributed to growing discontent in the weeks leading up to the Egyptian Revolution of 2011.

D Is Internet Access a Fundamental Right?

Even if the Internet is becoming increasingly important in this sector, only 20 percent of the population in these countries has access to Internet and only 5 percent are familiar with Facebook. It raises the question: Is Internet access a fundamental right?

Since the uprisings in the Arab world, increasingly more experts demand more human rights commitment for the Internet. The Special Rapporteur of the UN for the right to freedom of opinion and expression, Frank La Rue, came to the conclusion that the Internet now has a key position for the exercise of the freedom of expression under Article 19 of the Universal Declaration of Human Rights and as a catalyst for other human rights. Therefore, "to ensure universal access to the internet should be a be a priority for all nations."

Ironically, however, Vint Cerf, Chief Internet Evangelist for Google, argued that access to the Internet is not a human right. The Internet is only a means to an end; it could in itself constitute an inalienable right, because it is interchangeable in his eyes. Scott Edwards of Amnesty International accuses Cerf that this separation of means and ends is not philosophically coherent. In developing countries, the right to freedom of expression and free access to information are inherent to the law on Internet.

Without the weight of access to the Internet as a human right, it would be too easy for governments to restrict access to the Internet in times of crisis or stop altogether.

Gerhard Jandl

The Challenges of Cyber Security – a Government's Perspective

© BMeiA 2012

A Doctrinal Considerations

In recent years, many countries and international organizations have updated and revised their respective defense doctrines or security strategies. A common trend of these texts is the reference to the growing importance of the so-called new, emerging or unconventional security threats, ranging from terrorism to the implications of the financial crisis, from piracy to trans-border organized crime, from resources scarcity to the impact of climate change. Among these new challenges enumerated, cyber security usually figures very prominently. This is also true for the draft National Security Strategy of Austria which should replace the Security and Defense Doctrine dating from 2001.[1] The Austrian Federal Government approved the draft in March 2011, and conveyed it to Parliament for further consideration and eventual adoption as a Parliament Resolution (*Entschließung des Nationalrats*).[2] A special Sub-Committee of the Defense Committee was formed and has held several meetings to date. The opposition parties have proposed a number of amendments. At this juncture, though, it cannot be indicated yet when the new National Security Strategy will be adopted by the Parliament and thus will enter into force.

Various chapters of this draft specifically refer to cyber attacks, cyber criminality and the misuse of the Internet, and task the competent government agencies and ministries to continuously deal with this (and other relevant) items in their security-related activities. The draft also indicates the need for a comprehensive cyber security concept (see below).

For reasons of orientation, let's have a look at the respective provisions in the key strategic documents of EU and NATO. As regards the EU, cyber security is not

[1] Austrian Parliament, Resolution 114/E (XXI. GP), 12 December 2001.

[2] Austrian Parliament, *Report of the Federal Governent on the Austrian Security Strategy – Security in a New Decade: Developing Security (Bericht der Bundesregierung betr. Österreichische Sicherheitsstrategie. Sicherheit in einer neuen Dekade – Sicherheit gestalten)*, Doc. III-218 der Beilagen XXIV. GP. Available online at: http://www.parlament.gv.at/PAKT/VHG / XXIV/III/III_00218/index.shtml. (All websites used in this essay were last checked on 27 June 2012).

explicitly addressed in the European Security Strategy of 2003,[3] but in the High Representative's 2008 Report on the Implementation of the European Security Strategy – Providing Security in a Changing World:

> "*Modern economies are heavily reliant on critical infrastructure including transport, communication and power supplies, but also the Internet. The EU Strategy for a Secure Information Society, adopted in 2006 addresses Internet-based crime. However, attacks against private or government IT systems in EU Member States have given this a new dimension, as a potential new economic, political and military weapon. More work is required in this area, to explore a comprehensive EU approach, raise awareness and enhance international co-operation*."[4]

NATO's new Strategic Concept of 2010 treats the cyber area very prominently:

> "*Cyber attacks are becoming more frequent, more organized and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services,*

[3] European Union, *A Secure Europe in a Better World – European Security Strategy*, 12 December 2003.

[4] European Union, *Providing Security in a Changing World*, Report on the Implementation of the European Security Strategy, S407/08, 11 December 2008, at p. 5.

> *organized criminals, terrorist and/or extremist groups can each be the source of such attacks*."[5]

And it pledges to "develop further our ability to prevent, detect, defend against and recover from cyber attacks, including by using the NATO planning process to enhance and coordinate national cyber-defense capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations".[6]

The evolution of the language between 2003 and 2010 illustrates the growing importance of the cyber issue over the past years.

B The Austrian Draft National Security Strategy

Although this is not the place to discuss the contents of the draft National Security Strategy in detail,[7] a short sketch of the main lines might be useful. The document starts from the following considerations:

- traditional threats and challenges to security are becoming less imminent; new and more complex threats/challenges are becoming more important;
- the role of international organizations is growing, the role of state actors relatively declining;

[5] NATO, *Active Engagement, Modern Defense - Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization*, NATO Summit, Lisbon, 19-20 November 2010, 2010, at para. 12.

[6] NATO, *Active Engagement, Modern Defense - Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization*, at para.19.

[7] For a more detailed discussion, see Jandl, Gerhard, *Zur zeitgemäßen Aufgabe österreichischer Sicherheitspolitik*, in: Khol, Andreas, Günther Ofner, Stefan Karner and Dietmar Halper (eds.), *Österreichisches Jahrbuch für Politik 2011*, Böhlau Verlag, Vienna, 2012, at pp. 365 ff.

- a comprehensive approach according to the principle of comparative advantages of the respective actors is needed on the international and regional levels;
- a more interactive and integrated approach (civilian/military) is needed on the domestic level (the so-called "whole of government approach");
- security increasingly also comprises economic, social, development and interior security aspects (which is why the draft National Security Strategy contains detailed language also on domestic security issues).

The draft National Security Strategy commends the new role of the post-Lisbon Treaty EU in crisis management, including the clause which requires Member States to improve their capabilities and make them available to the EU. It welcomes NATO's Strategic Concept of 2010, including NATO's increased ambitions in international crisis management, in cooperative security, in tackling new security challenges, and in the upgrading of its partnerships.

According to the draft National Security Strategy, Austria will craft its security policy mainly in the frameworks of the UN, the EU, the OSCE and NATO partnerships. It pledges continued Austrian cooperation within and with these organizations, and Austrian contributions to their respective endeavors. Participation in international crisis management missions/operations is understood as an essential element of this policy. Crisis prevention, mediation and the support of disarmament measures are further important elements.

Defense policy is defined as an integral part of the Comprehensive Security Provision (*Umfassende*

Sicherheitsvorsorge),[8] as being required to cooperate with internal security and foreign policies, and as comprising: the defense of sovereignty and territorial integrity; the protection of constitutional institutions and critical infrastructure (a supporting role to the organs of domestic security); the protection of the population, including in case of natural disasters; a contribution to ensuring the functioning of the state institutions; the participation in international crisis management; and a contribution to the EU's security policy. Emerging security challenges can lead to new tasks for the Austrian armed forces and other official institutions and bodies.

C Particular Challenges from a Government – and a Personal – Perspective

Turning now to the challenges for government reaction to the said risks, let me say a few words from the background of my position as Security Policy Director, though with a personal underpinning.

Let's embark from the observation that the changes and advances in technology, in particular in IT technology, are not happening at a "bureaucratic" pace, but exponentially faster. One has only to mention inventions like Twitter, Facebook, Cloud Computing, and others. Risks and dangers involved are growing by the same speed as the innovations themselves. This puts governments in a very difficult situation. Not only because state administrations are, more or less by definition, slower than innovative industries. But also because state action – or rather reaction – must (a) be based on a broad political consensus of, at least, the parliamentary majority,

[8] On the current defense policy strategy, see: Austrian Ministry of Defence *Teilstrategie Verteidigungspolitik*, 2010. Available online at: http://www.bmlv.gv.at/facts/bh_2010/archiv/pdf/teilstrategie_vertpol.pdf.

preferably though on that of a much wider societal majority; and (b) must – both in the process of its elaboration and in its contents – respect the fundamental principles of our society, such as the rule of law, the separation of powers, the individual freedoms, etc. Such processes obviously take time.

Why did I say "rather reaction than action" when it comes to the role of the state? This is not to advocate the state having a passive, reactive role in general – far from it. Rather, the word "reaction" seems to be a better notion than "action" because freedom of opinion, freedom of expression, freedom of information are values of such paramount importance that state authorities must not interfere here, unless in circumstances under which it is absolutely inevitable. I take it that these considerations and convictions are being equally shared by – hopefully – many if not all decision makers in democratic and liberal societies.

When, hence, is such state intervention inevitable? One can see a number of cases – the clustering of which is basically geared to the cutting-edge discussion at the 2011 Munich Security Conference:[9]

- When IT technology is used for criminal purposes – cyber crime in other words. For example, the use of Internet means to illegally transfer money, to steal money from other peoples' bank accounts, to carry out industrial espionage, to spread or consume child pornography etc. The required state action consists, in my view, in the elaboration and implementation of appropriate penal norms.

[9] See e.g.: Habig, Cornelia, *Der Cyberspace stellt die Welt vor komplexe Herausforderungen*, 5 February 2011. Available online at: http://www.securityconference.de/TOP-NEWS.638+M59693ca518f.0.html.

- When the Internet is used for the radicalization of people, that is when hate speech is being spread, intolerance and violent or terrorist activities against other nations, races or followers of different belief or conviction, is being incited and the formation of groups for such purposes is being attempted. The required state action here is a combination of inhibiting such contents with, again, the elaboration and implementation of appropriate penal norms.
- When IT technology is used for so-called cyber attacks,that is for attacks on the very existence and fundamental safety of our countries, economies and societies. Attacks designed, for example, to bring down the electricity distribution, the health system, the financial and commercial infrastructure or the defense system on such a large scale that public life cannot continue to function properly or that national security is at stake. In those cases, the state must see to it that its crucial networks are safe and resilient and must constantly update the relevant protection measures.

It is obvious that no single ministry or even single government agency can fulfill these tasks alone. A "whole-of-government" approach or, indeed, a "whole-of-nation" approach involving also private stakeholders is required. Furthermore, no single country can successfully act just by itself. International cooperation becomes more and more pivotal, including with relevant international organizations that play an ever increasing role. This fact, by the way, is underlined in practically all recent doctrinal documents of states and international organizations.

D The Austrian Response, Nationally…

Let me now give you a short overview over what has been going on Austrian government level in the cyber security area. The well-developed national crisis response mechanisms and structures are being utilized to meet also new challenges such as cyber security. The coordination competence rests with the Federal Chancellery, which has established a government Computer Emergency Response Team (CERT) in 2008 in order to integrate cyber security efforts of the public and private sectors. The Federal Chancellery coordinates cyber crisis management with other government, CERT stakeholders and in consultation with experts from the Ministries of Interior and Defence. In 2010, the "Internet Offensive Austria" – a joint initiative of the ICT stakeholders of Austria (leading local ICT companies, research institutions and interest groups) – developed a national ICT strategy, the “Austria Internet Declaration”. Moreover, government has set up a Center of Excellence for the Internet Society, which uses this Declaration as a comprehensive guideline for the future “whole-of-government” approach.

At present, a number of cyber security related initiatives are ongoing in Austria. In particular:

- At the initiative of the Federal Chancellery and CERT.at, an Austrian Trust Circle was founded as a multi-sectoral platform of ICT security experts from the private sector. This platform will play an essential role, in particular by providing crisis management capabilities for the local infrastructure against cyber security threats. A number of expert groups have already been established for various sectors, such as finance and health care.
- A number of research projects on cyber threats have been identified and started.

- Austria has set up a Private Public Partnership Program for Critical Infrastructure Protection (APCIP) with the objective to develop a comprehensive strategy and detailed measures and to bring all relevant public and private organizations and infrastructure operators under one common conceptual roof.
- The Defense Ministry is further developing its cyber defense capabilities by setting up a military CERT.
- The Interior Ministry has started to elaborate a Cyber Risk Matrix and Analysis, involving the academic, business, administration and political communities.

The individual activities carried out by various ministries and agencies will be consolidated by a future national cyber security concept, as mentioned by the draft National Security Strategy. Preparatory works within the Secretariat of the National Security Council have begun recently, and it is foreseen to set up such a structure within the first half of 2012.

E …and Internationally

Austria has also been promoting the issue of cyber security in different international organisations.

In OSCE, Austria is among a group of Participating States promoting cyber security issues within that organization. In particular, it advocates the development of Confidence and Security Building Measures (CSBMs) and training activities in field missions.

In the Council of Europe, Austria holds the position of Thematic Coordinator on Information Policy Internet Governance, playing an important role in drafting the new Council of Europe Strategy on Internet Governance 2012

– 2015 which involves NGOs and puts particular emphasis on compliance with Human Rights.[10]

But perhaps most importantly, Austria and NATO – the latter being the very organization most advanced in the cyber field[11] – have commenced a comprehensive bilateral cooperation scheme on all relevant aspects of cyber security. Austria has been the first country (not only partner country) ever to start such collaboration, under the aegis of NATO's newly established Emerging Security Challenges Division, in the fall of 2011.[12] To date, half a dozen other states have followed this example.

A number of possible areas of cooperation have been identified: harmonization of crisis management procedures; exchange of relevant information and assessments; mutual inclusion in research projects; joint mentorships in third countries to raise awareness; development of joint "lessons learned" processes, including on cyber aspects of crisis management operations; establishment and enhancement of cyber security related capabilities and procedures; training and exercises (including at the NATO Cooperative Cyber Defense Center in Tallinn); and the involvement of the private sector, as appropriate.

[10] See: Council of Europe, Information society and Internet governance, *"Our Internet - Our Rights, Our Freedoms": Towards the Council of Europe Strategy on Internet Governance 2012-2015*, 2011. Available online at: http://www.coe.int/t/informationsociety/conf2011/.

[11] See NATO, *NATO and Cyber defence*, 2012. Available online at: http://www.nato.int/cps/en/natolive/topics_78170.htm?.

[12] On the event launching that cooperation, see e.g.: Kurier, „Cyber-Sicherheit: NATO spricht mit Österreich", 4 November 2011. On Austria's partnership with NATO in general, see NATO, *NATO's relations with Austria*, 2012. Available online at: http://www.nato.int/cps/en/SID-F47CD065-4BB3E8E8/natolive/topics_48901.htm.

Moreover, Austria has been actively participating in the implementation of NATO’s Cyber Policy and Action Plan, insofar as it is open to partners. NATO has suggested the inclusion of a number of cyber security related projects in the Individual Partnership Cooperation Program (IPCP) and the Planning and Review Process (PARP) – the two main cooperation instruments for partners like Austria – and it is certainly hoped that this proposal will be implemented swiftly.

II Balancing Law, Technology and Human Rights

Farhan Sahito[*] and Wolfgang Slany[**]

Functional Magnetic Resonance Imaging and the Challenge of Balancing Human Security with State Security

Abstract

Recent reports reveal that violent extremists are trying to obtain insider positions that may increase the impact of any attack on critical infrastructure and could potentially endanger state services, people's lives and even democracy. It is of utmost importance to be able to adopt extreme security measures in certain high-risk situations in order to secure critical infrastructure and thus lower the level of terrorist threats while preserving the rights of citizens. To counter these threats, our research is aiming for extreme measures to analyse and evaluate human threats related assessment methods for employee screening and evaluations using cognitive analysis technology, in particular functional Magnetic Resonance Imaging (fMRI). The development of fMRI has led some researchers to conclude that this technology has forensic potential and may be useful in investing personality traits, mental illness, psychopathology, racial prejudice and religious extremism. However, critics claim that this technology may present many new human rights and ethical dilemmas and could result in potentially disastrous outcomes. The main thrust of the research is to counter above concerns and harmful

[*] Master's Degree in Criminology from University of Melbourne, Australia, currently a PhD candidate in cyber crime at the Institute for Software Technology at Graz University of Technology, Austria. The author can be contacted by email at: fsahito@ist.tugraz.at.

[**] Professor and head of the Institute for Software Technology at Graz University of Technology, Austria. The author can be contacted by email at: wolfgang.slany@tugraz.at.

consequences by presenting a set of ethical and professional guidelines that will substantially reduce the risk of unethical use of this technology. The significance of this research is to ensure the limits of the state/organisation's right to peer into an individual's thought process with and without consent, to define the parameters of a person's right to ensure that fMRI scans do not pose more than an appropriate threat to cognitive liberty, and the proper use of such information in civil, forensic and security settings.

Keywords: fMRI, Critical Infrastructure, Employee Screening, Human Security, State Security

A Introduction

September 11th has marked an important turning point that exposed new types of security threats and disclosed how terrorists' pursuit of their long-term strategic objectives includes attacks on innocent civilians and critical infrastructures that could result in not only large-scale human casualties but also profound damage to national power and prestige[1]. Recent reports[2] also reveal that violent extremists are trying to obtain insider positions in critical infrastructure. Based on these reports, it is clear that their actions pose a significant threat. States have an extreme interest in detecting malicious insiders and may in certain cases take extreme measures to assure the protection of critical infrastructure and services within their

[1] Birkett, Dave, Jim Truscott, Helena Mala-Jetmarova and Andrew Baarton, *Vulnerability Of Water And Wastewater Infrastructure And Its Protection From Acts Of Terrorism: A Business Perspective*, in: Clark, Robert M., Simon Hakim and Avi Ostfeld (eds.), *Handbook Of Water And Wastewater Systems Protection*, Springer, USA, 2011.

[2] US Department of Homeland Security, *Insider Threats To Utilities*, 2011. Available online at: http://info.public intelligence.net/DHS-InsiderThreat.pdf (All websites used in this essay were last checked on 18 June 2012).

jurisdictions while preserving the rights of citizens. Despite much investigation into the motivation and psychology of malicious insiders, the fact remains that it is extremely complicated to predict insider motivation[3]. This presents operators of critical infrastructure with a dilemma to establish an appropriate level of trust w.r.t. employees.

The purpose of our research is to alleviate these threats by focusing on a multi-layered security strategy such as training of employees, threat management, security awareness policies and employees screening. However, the main thrust of this paper is centred on extreme measures such as employee screening on critical positions using cognitive analysis technology, in particular functional Magnetic Resonance Imaging (fMRI). Proponents of this neuro-imaging technology hailed fMRI as the next “truth meter” and conclude that because of the novelty of the physiological parameters being measured, this technology may be more accurate than other traditional methods for employee screening (e.g., polygraph[4]).The hallmark of this study is to use fMRI technology to protect critical infrastructure, by providing an acceptable level of assurance as to the integrity of

[3] Brancik, Kenneth and Gabriel Ghinita, *The Optimization Of Situational Awareness For Insider Threat Detection*, in: Ravi S, Sandhu and Elisa Bertino (eds.), CODASPY, ACM, 2011, pp. 231-236. Available online at: http://dl.acm.org/citation.cfm?id=1943544.

[4] See Bruni, Tommaso, *Cross-Cultural Variation And fMRI Lie-Detection*, in: Van den Berg, B. and L. Klaming (eds.), *Technologies On The Stand: Legal And Ethical Questions In Neuroscience And Robotics*, Wolf Legal Publishers, Nijmegen, 2012, pp. 129-148; Faulkes, Zen, *Can Brain Imaging Replace Interrogation And Torture?,* Global Virtue Ethics Review (Volume 6, Issue 2), 2011, pp. 55-78; McCabe, David P, Alan D. Castel and Matthew G. Rhodes, *The Influence Of fMRI Lie Detection Evidence On Juror Decision-Making*, Behavioral Sciences and the Law (Volume 29), 2011, pp. 566-577.

individuals who have access to sensitive information or/and who require access to key assets, individuals, protectively marked state's data and material, at risk of terrorist attacks. The aim is to establish an appropriate level of trust of employees, effective monitoring and ensuring that insiders do not pose a foreseeable risk to critical infrastructure. Eliminating or reducing the likelihood of deception could lighten the burden of suspicion and mistrust to promote state security and secure human lives. Clearly this is an area of great sensitivity so we need to understand that threats to critical infrastructure are becoming increasingly frequent.

To sum up, this research examines the use of fMRI technology in critical infrastructure security. The aim of our research is to show that neuro-imaging can be an important, helpful, and successful tool for state security from an employee screening perspective. However, despite the intriguing results of many studies, there are several concerns which must be addressed prior to moving this technology to real-world application[5]. For some critics, the issues of legal, ethical and privacy violations that may clash with questions of state security and human security may raise with this technology. The significance of this research is to ensure that maintaining human security is as important as promoting state security. This paper will not discuss the methodology of implementing this technology; instead the focus will be on addressing the research challenges and related issues and to elucidate our method that includes monitoring of employee to predict or detect insider threats. We show that these methods are helpful and productive and could alleviate the burden of mistrust and increase the efficiency

[5] Garnett, Alex, Louise Whiteley, Heather Piwowar, Edie Rasmussen and Judy Illes, *Neuroethics And fMRI: Mapping A Fledgling Relationship*, PLoS ONE (Volume 6, Issue 4), 2011.

of threat avoidance measures. More importantly, we discuss the pros and cons of this neuro-imaging technique to ensure that both state security and human security are balanced in order to achieve the objectives of this research and that it does not lead to the conclusion that the use of this technology for employee screening is ethically dubious.

B Malicious Insiders in Critical Infrastructure: A Threat to State Security

Critical infrastructures are the advanced physical and cyber-based systems essential to the state's security, economic prosperity and social well-being of the nation, such as law enforcement services, power plants and information and communication services etc[6]. As a result of advances in technology, these critical infrastructures have become increasingly automated and interlinked. On the other side, these advances have created new vulnerabilities to physical and cyber attacks by insiders[7]. The study "Cost of Data Breach Study: United States" from 2011 reveals that insiders are the top cause of data breaches and 25 percent more costly than other types[8].

[6] Moteff, John D., *Critical Infrastructures: Background, Policy, And Implementation*, CRS Report for Congress, RL30153, Congressional Research Service, Washington, D. C, 2011.

[7] Noonan, Thomas and Edmund Archuleta, *The National Infrastructure Advisory Council's Final Report And Recommendations On The Insider Threat To Critical Infrastructures*, 2008. Available online at: http://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf.

[8] Symantec, *Ponemon Cost Of A Data Breach*, nd. Available online at: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon&om_ext_cid=biz_socmed_

Moving data and application in IT brings with it an inherent level of risk that allows insiders to steal confidential data such as passwords and cryptographic keys, sabotage information resources as well as various types of frauds[9]. These threats carry debilitating impact on state's defence and economic security, including a loss of public confidence in state's services that would seriously undermine public safety and the fulfilment of key government responsibilities[10].

A new report[11] issued by the US Department of Homeland Security uncovers that malicious insiders and their actions pose a significant threat to critical infrastructure in the USA and the world, and may increase the impact of any attack on critical infrastructure. According to this report, the fall edition of AQAP (a magazine published by al-Qaeda) encourages followers to use "*specialized expertise and those who work in sensitive locations that would offer them unique opportunities*" to conduct terrorist attacks in the world. The US authorities were stunned in 2009 in Yemen with the arrest of an alleged American recruit to al-Qaeda, Sharif Mobley, who had been employed at five different US nuclear power plants in and around Pennsylvania after successfully

twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach.

[9] Matthew, Asha, *Security And Privacy Issues Of Cloud Computing; Solutions And Secure Framework*, International Journal of Multidisciplinary Research (Volume 2, Issue 4), 2012, pp. 182-193.

[10] Jackson, James K., *Foreign Investment And National Security: Economic Considerations*, CRS Report for Congress, RL34561, Congressional Research Service, Washington, D. C., 2011. Available online at: http://www.fas.org/sgp/crs/natsec/RL34561.pdf.

[11] US Deparment of Homeland Security, *Insider Threats To Utilities*, 2011.

passing federal background checks[12]. The sequence of scandals induced by the 2010 as publication of classified government documents to the Wiki-Leaks website[13] – in which volumes of sensitive documents were leaked by a trusted insider and ultimately published on an open website – has caused much embarrassment to the United States and other nations and represents the ultimate nightmare scenario for governments when considering the human aspect in critical infrastructure.

It is indeed sobering to imagine that any organisation could fall victim to such events and the damage malicious insider can do. The US president issued an executive order in October 2011[14] to create an Insider Threat Task Force to prevent potentially damaging and embarrassing exposure of important secrets. Eugene Spafford, executive director of Purdue University's Centre for Education and Research in Information Assurance and Security, said the president's action was long overdue: "*Why haven't they been doing this already? This is at least 10 years too late, if not 20*[15]. " It is indeed sobering to imagine that any critical infrastructure could fall victim to such events and the damage malicious insider can do.

[12] Sharp, Jeremy M., *Yemen: Background And U.S. Relations* CRS Report for Congress, RL34561, Congressional Research Service, Washington, D. C., 2011. Available online at: http://www.fas.org/sgp/crs/mideast/RL34170.pdf.

[13] Fenster, Mark, *Disclosure's Effects: Wikileaks And Transparency*, Iowa Law Review (Volume 97), 2012, pp. 11-56.

[14] The White House – Office of the Press Secretary, *Structural Reforms To Improve The Security Of Classified Networks And The Responsible Sharing And Safeguarding Of Classified Information*, 2011. Available online at: http://docs.govinfo security.com/files/external/2011wiki_eo_rel.pdf.

[15] GovInfoSecurity, *Obama Establishes Insider Threat Task Force*, 2011. Available online at: http://www.govinfosecurity.com/articles.php?art_id=4136.

C Malicious Insiders in Critical Infrastructure: Why We Cannot Stop Them?

The "insider" is an individual authorized to access an organisation's information system, network or data — based on trust[16]. The insider threat refers to harmful acts and malicious activities that trusted insiders might carry out such as negligent use of classified data, unauthorized access to sensitive information, fraud, illicit communications with unauthorized recipients and something that causes harm to the organisation[17]. Insiders can be system administrator, contractors, former employees, suppliers, security guards and partner employees etc. According to Noonan and Archuleta[18] malicious insiders can be labelled as three different types of actors: 1) criminals 2) ideological or religious radicals; and 3) psychologically-impaired disgruntled or alienated employees. The motivation of malicious insider can be summarized as simple illicit financial gain; revenge for a perceived wrong; or radicalization for advancement of religious or ideological objectives. Insider threats are often cited as the most serious security problem difficult to deal with as he/she has capabilities and information not known to external attackers. Governments are taking all

[16] Greitzer, Frank L., Andrew P. Moore, Dawn M. Cappelli, Dee H. Andrews, Lynn A. Carroll and Thomas D. Hull, *Combating The Insider Cyber Threat*, IEEE Security and Privacy (Volume 6, Issue 1), 2008, pp. 61-64.

[17] Sun, Yuqing, Ninghui Li and Elisa Bertino, *Proactive Defence Of Insider Threats Through Authorization Management,* in: Proceedings of 2011 International Workshop on Ubiquitous Affective Awareness and Intelligent Interaction (UAAII '11), ACM, New York, 2011, pp. 9-16. Available online at: http://dl.acm.org/citation.cfm?id=2030095.

[18] Noonan and Archuleta, *The National Infrastructure Advisory Council's Final Report And Recommendations On The Insider Threat To Critical Infrastructures*, 2008.

necessary measures to swiftly eliminate any significant threat from internal vulnerabilities on their critical infrastructures as such damage would generally be catastrophic and far-reaching – such as terrorist attacks[19], but the extent to which this can be done at all is far from sufficient.

To counter human threats, agencies have invested billions of Euros in different technical measures for years now[20]. The current security paradigms include access control and encryption to face malicious insiders and outsiders. They are implemented through passwords, physical token authentication and biometric authentication, firewalls, encrypted data transmission, data leakage prevention, behavioural-pattern threat detection, voice stress analysis and polygraphs. Some significant techniques that are being used to mitigate particularly human factors by critical organisations include:

> ***1. Biometrics:*** Biometrics refers to technologies that measure human body characteristics, such as voice patterns, fingerprints, DNA, retina and iris patterns, facial patterns and hand measurements, for authentication purposes. However, according to security experts this technology has not yet produced concrete results in providing scalable solutions in detecting insider and outsider threats to critical organisations and comes with an

[19] Chiaradonna Silvano, Felicita di Giandomenico and Paolo Lollini, *Evaluation Of Critical Infrastructures: Challenges And Viable Approaches*, Lecture Notes in Computer Science (Volume 5135), 2008, pp. 52-77.

[20] Sarka, Kuheli Roy, *Assessing Insider Threats To Information Security Using Technical, Behavioural And Organisational Measures*, Information Security Technical Report (Volume 15, Issue 3), 2010, pp. 1-22.

associated error probability[21]. According to Jim Wayman, former director, US Government Biometrics Center, "*it really isn't for security — it's for convenience*"[22]. These technologies increase risks to personal privacy and security of employees with no commensurate benefit for performance. Computers are fast at computation but not very good at judgment and expert social engineers can easily fool these devices[23].

2. Proximity badges: A badge worn by an employee that can be sensed by his or her work place. A workstation might be set to lock up if an authorised user's presence is not sensed. The issue is that not all proximity badges are in fact secure. Proximity badges are a perfect attack goal for social engineers as they provide a false sense of security while being very easy to steal and/or substitute[24].

[21] Sandhu, Parvinder S, Iqbaldeep Kaur, Amit Verma, Samriti Jindal and Shailendra Singh, *Biometric Methods And Implementation Of Algorithms*, International Journal of Electrical and Electronics Engineering (Volume 3, Issue 8), 2009, pp. 3-8.

[22] Gutman, Peter, *Why Biometrics Is Not A Panacea*, nd. Available online at: http://www.scribd.com/doc/3099277/Why-Biometrics-is-not-a-Panacea.

[23] Best Jr, Richard A., *Intelligence Information: Need-to-Know vs. Need-to-Share*, CRS Report for Congress, RL41848, Congressional Research Service, Washington, D. C, 2011. Available online at: http://www.fas.org/sgp/crs/intel/R41848.pdf.

[24] Anderson, Robert H., *Research And Development Initiatives Focused On Prevention, Detecting, And Responding To Insider Misuse Of Critical Defense Information Systems*, RAND Conference Proceedings (CF151), 2005. Available online at: http://www.rand.org/pubs/conf_proceedings/2005/CF151.pdf. See also Department of Defense, *Final Report Of The Insider Threat Integrated Process Team*, Washington D.C., 2000.

3. Access control software: This technique is used to implement least privilege policies for users and locks a system after an idle period, requiring a password to reinstate the display. A significant insider vulnerability is the unattended, yet logged-in system. According to several studies least privilege is often difficult or costly to achieve because it is difficult to tailor access based on various attributes or constraints[25].

4. Frequent or periodic re-authentication during a user access session: This approach is also used by various organisations to preventing an insider from masquerading as another legitimate user in the presence of a personal "token", e.g., a smart card during a session; however, various reports of breaches in the security system acknowledged that this system is not a fool-proof mechanism[26].

5. Voice stress analysis (VSA): Some organisations and law enforcement agencies also use voice stress analysers to determine if, e.g., a caller or employees is lying. This technology is said to record physiological stress responses that

Available online at: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA391380.

[25] Bowen, Brian M., Malek Ben Salem, Angelos D. Keromytis and Salvatore J. Stolfo, *Monitoring Technologies For Mitigating Insider Threats In Cyber Security And Beyond*, 2009. Available online at: http://ids.cs.columbia.edu/sites/default/files/insider-bookchapter.pdf.

[26] Li, Chun-Ta, Cheng-Chi Lee, Chen-Ju Liu and Chin-Wen Lee, *A Robust Remote User Authentication Scheme Against Smart Card Security Breach*, Lectures Notes in Computer Science (Volume 6818), 2011, pp. 231-238.

are present in the human voice in the Detection of Deception (DOD) scenario. The monetary costs are substantial: it can cost up to €20,000 to purchase VSA technology. However, several studies conducted on the reliability of computer voice analysers to detect deception showed "little validity" in the technique[27].

6. Polygraph: The Polygraph method aims at determining physiological correlates of behaviour such as a set of physiological parameters. Polygraph measures the subject's psychological response by monitoring blood pressure, pulse, chest expansion and electrical conductance of the skin that mirrors the activity of the autonomic nervous system in order to detect anxiety and deception in the subject[28]. However, there have been ongoing concerns and debate over polygraph's accuracy and reliability of measurement. This conventional device also raises ethical and legal issues and the relevance of the test to the field situations (e.g., civil and judicial settings) in which it is used[29]. As a result, lives may be ruined and shattered with this technology. Maher Arar, a Canadian citizen who was born in Syria is one example of a victim of the

[27] Eriksson, Anders and Francisco Lacerda, *Charlatanry In Forensic Speech Science: A Problem To Be Taken Seriously*, International Journal of Speech, Language and the Law (Volume 14, Issue 2), 2007, pp. 169-193.

[28] McCabe, David P., Alan D. Castel and Matthew G. Rhodes, *The Influence Of fMRI Lie Detection Evidence On Juror Decision-Making*, Behavioral Sciences and the Law (Volume 29), 2011, pp. 566-577.

[29] Simpson, Joseph R., *Functional MRI Lie Detection: Too Good To Be True?*, Journal of the American Academy of Psychiatry and the Law Online (Volume 36, Issue 4), 2008, pp. 491-498.

> technology. In September 2002 when he was returning to Canada with his family from Tunisia he was detained by U.S. officials while changing planes at New York airport. After 13 days of questioning with polygraph (but no court action or formal action), he was handed over to Syrian law enforcement. After torture and one year of imprisonment he was released through Canadian intervention. The Canadian government apologized to him in 2007 (after a two year study by a prestigious commission[30]) and agreed to pay him 9 million U.S. dollars. However, the United States government has not apologized[31]. On the other hand, it is very easy to cheat polygraphs, and a simple internet search of polygraph counter measures can reveal many ways how to cheat this technology. One former polygrapher also charges $59.95 for his manual plus DVD offering information on beating the polygraph[32].

Various studies demonstrate that above devices and security software are normally designed to defend against external threats to secure critical infrastructure and do not protect against attacks aided by internal help in organisations. An insider not only has the ability to obtain

[30] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report Of The Events Relating To Maher Arar: Factual Background*, vol II, 2006. Available online at: http://www.sirc-csars.gc.ca/pdfs/cm_arar_bgv2-eng.pdf.

[31] Macklin, Audrey, *From Cooperation, To Complicity, To Compensation: The War On Terror, Extraordinary Rendition, And The Cost Of Torture*, European Journal of Migration and Law (Volume 10, Issue 1), 2008, pp. 11-30, at p. 17.

[32] Greely, Henry T. and Judy Illes, *Neuroscience-based Lie Detection: The Urgent Need For Regulation*, American Journal of Law and Medicine (Volume 33, Issue 2-3), 2007, pp. 377-431.

or access valuable data that resides on the internal network, but he/she can obtain this data from their workstation without causing suspicion or breaking trust. With unjustified trust, people cannot keep faith in state capability if the information is not assured and safe. Christopher Porter wrote that "*Security technology is not a panacea. It's a process of which technology is only a piece of the puzzle*"[33]. Any security system, no matter how well designed and implemented, will have to rely on people. Technology can be used as a control, but not in isolation as it is relatively simple for a social engineer to persuade one of the critical employees to divulge their log-in details, or for a malicious insider with legitimate access to abuse his/her position. We can implement appropriate technical solutions, but we still fail to handle the human factor. According to Kevin Mitnick, one of the most notorious social engineers, the human side of security is easily exploited and constantly overlooked. Agencies spend millions of Euros on firewalls, encryption and secure access devices, and it is often money wasted when none of these measures address the weakest link in the security chain, namely people[34].

Employees at all levels of the organisation are important to the overall protection strategy for critical infrastructure. Without all employees being part of the team, the enterprise, its assets, and its employees will be open to attack from malicious insiders[35]. Critical infrastructures

[33] Security Blog, *Security Can Not Be Addressed By Technology Alone*, 2010. Available online at: http://securityblog.verizonbusiness.com/2010/12/06/security-can-not-be-addressed-by-technology-alone/.

[34] Mitnick, Kevin D. and William L. Simon, *The Art Of Intrusion: The Real Stories Behind The Exploits Of Hackers, Intruders & Deceivers*, Wile, New York, 1995.

[35] Cappelli, Dawn, Andrew Moore, Randall Trzeciak and Timothy J. Shimeall, *Common Sense Guide To Prevention And Detection Of Insider Threats* (3rd Edition, Version 3), CERT,

would not likely fill an employee position of such gravity without conducting a background investigation and constant screening as employees at critical positions may be, in some instances, the first and only line of defence, and thus vital to national security. It very frequently would be of utmost importance to adopt extreme measures to secure critical infrastructure in order to lower the level of threats while preserving the rights of citizens. To the best of our knowledge, no single current approach solves this problem.

D Maintaining Security using Functional Magnetic Resonance Imaging (fMRI)

To overcome above limitations, researchers recently have attempted to use brain fingerprinting or brain scanning technologies to detect insider threats. Eck (1970)[36] argues that "*Every generation has attempted to develop objective and reproducible methods to discover the truth*". Similarly, due to the inherent limitations of above technologies such as polygraph, it is not surprising that research communities and intelligence personnel have started recognizing that medical science — in particular, fMRI — may have potential applications in economics contexts, justification of cognitive enhancing drugs in educational settings, detecting deception, interrogation process and be effective in courtroom situation[37]. For instance, in September 2008, a court in India allowed to use brain scan images in a criminal case. Aditi Sharma was convicted by a court for the murder of her former fiancé,

2009. Available online at: http://www.cert.org/archive/pdf/CSG-V3.pdf.

[36] Eck, Marcel, *Lies and Truth*, Macmillan, New York, 1970.

[37] Garnett *et al*, *Neuroethics And fMRI: Mapping A Fledgling Relationship*, 2011.

Udit Bharati. However, for the first time, a brain scan was used as evidence of a criminal defendant's guilt. This case marked the dawn of a new era for the use of brain scan technology in criminal prosecution. The court found that the brain scan proved that Aditi Sharma had experimental knowledge of having murdered Udit Bharati herself[38]. A variety of recent advances in neurological research and the development of this new technology claim to be a more accurately deception revealing tool for screening purposes and in counterterrorism investigations, that can be effective in distinguishing truth tellers from liars and to determine hidden conscious states of an individual, with accuracy greater than chance[39]. In this research we argue that this information can be used as a tool warranted for certain extremely critical employment situations to secure key assets — as in this era of terrorism that is creating an all-pervasive fear, fMRI can be considered as a magic bullet in the war on terror.

fMRI is an increasingly popular neuro-imaging technique that was developed in the 1990s and has since become the preferred method for studying the functional anatomy of the human brain. This technique relies on the fact that cerebral blood flow and neuronal activation are coupled. When an area of the brain is in use, blood flow to that region also increases[40]. This is how the fMRI detects this physiological change due to the blood-oxygen-level-dependent, or BOLD, effect. In clinical settings, fMRI has been applied ranging from language comprehension to

[38] Brown, Teneille and Emily R. Murphy, *Through A Scanner Darkly: The Use of fMRI As Evidence of Mens Rea*, Journal of Law & Health (Volume 22, Issue 2), 2009, pp. 319-341.

[39] Faulkes, *Can Brain Imaging Replace Interrogation And Torture?*, 2011.

[40] Simpson, *Functional MRI Lie Detection: Too Good To Be True?*, 2008.

personality traits (happiness, sadness, fear, and anger), aesthetic judgment or political behaviour[41].

Since an initial publication in 2001 by Spence and his colleagues[42] on fMRI deception detection, several research papers and studies on the fMRI technique have reported experiments in which subjects were asked to deceive or lie in one task and respond truly in another task[43]. In these two studies, subjects were instructed to say yes when the truth is no and vice versa. In another study, the task paradigm included spontaneous lies[44], for instance, the subject was instructed to say Chicago when the truthful answer is Seattle. Similarly, Lee et al., 2002[45] and Lee et al., 2005[46] studies were included feigning memory impairment tasks. In addition, lying about having

[41] Garnett *et al*, *Neuroethics And fMRI: Mapping A Fledgling Relationship*, 2011.

[42] Spence, S .A., T.F. Farrow, A.E. Herford, I.D. Wilkinson and P.W. Woodruff, *Behavioral And Functional Anatomical Correlates Of Deception In Humans*, Neuroreport (Volume 12, Issue 13), 2001, pp. 2849-2853.

[43] Nuñez, Jennifer Maria, B.J. Casey, Tobias Egner, Todd Hare and Joy Hirsch, *Intentional False Responding Shares Neural Substrates With Response Conflict And Cognitive Control*, Neuroimage (Volume 25, Issue 1), 2005, pp. 267-277.

[44] Ganis, G., S.M. Kosslyn, S Stose, W.L. Thompson and D.A. Yurgelun-Todd, *Neural Correlates Of Different Types Of Deception: An fMRI Investigation*, Cerebral Cortex (Volume 13, Issue 8), 2003, pp. 830-836.

[45] Lee, Tatia M. C., Ho-Ling Liu, Li-Hai Tan, Chetwyn C.H. Chan, Srikanth Mahankali, Ching-Mei Feng, Jinwen Hou, Peter T. Fox and Jia-Hong Gao, *Lie Detection By Functional Magnetic Resonance Imaging*, Human Brain Mapping (Volume 15), 2002, pp. 157-164.

[46] Lee, Tatia M. C., Ho-Ling Liu, Chetwyn C.H. Chan, Yen-Bee Ng, Peter T. Fox and Jia-Hong Gao, *Neural Correlates Of Feigned Memory Impairment*, Neuroimage (Volume 28, Issue 2), 2005, pp. 305-313.

a play card (Langleben et al., 2005[47] and Davatzikos et al., 2005[48] and lying about having fired a gun[49] revealed that particular spots in the brain's prefrontal cortex become more active when a subject is suppressing the truth or lying. In some of the other experimental tasks, subjects were motivated by monetary incentives as they were told that they would double their reward money if they were able to deceive the fMRI machine, such as lying about having taken a ring or a watch[50] and lying about the place of hidden money[51].

In these experiments, this technology has been claimed to be 90% accurate by these researchers. In one study,

[47] Langleben, Daniel D., James W. Loughead, Warren B. Bilker, Kosha Ruparel, Anna Rose Childress, Samantha I. Busch and Ruben C. Gur, *Telling Truth From Lie In Individual Subjects With Fast Event-related fMRI*, Human Brain Mapping (Volume 26), 2005, pp. 262-272.

[48] Davatzikos, Christos, Kosha Ruparel, Yong Fan, Dinggang Shen, M. Acharrya, James. Loughead, Ruben Gur and Daniel D. Langleben, *Classifying Spatial Patterns Of Brain Activity With Machine Learning Methods: Application To Lie Detection*, Neuroimage (Volume 28, Issue 3), 2005, pp. 663-668.

[49] Mohamed, Feroze B., Scott H. Faro, Nathan J. Gordon, Steven M. Platek, Harris Ahmad and J. Michael Williams, *Brain Mapping Of Deception And Truth Telling About An Ecologically Valid Situation: Functional MR Imaging And Polygraph Investigation: Initial Experience*, Radiology (Volume 238, Issue 2), 2006, pp. 679-688.

[50] Kozel, F. Andrew, Kevin J. Johnson, Qiwen Mu, Emily L. Grenesko, Steven J. Laken and Mark S. George, *Detecting Deception Using Functional Magnetic Resonance Imaging*, Biological Psychiatry (Volume 58, Issue 8), 2005, pp. 605-613.

[51] Kozel, F. Andrew, Letty J. Revell, Jeffrey P. Lorberbaum, Ananda Shastri, Jon D. Elhai, Michael David Horner, Adam Smith, Ziad Nahas, Daryl E. Bohning and Mark S. George, *A Pilot Study Of Functional Magnetic Resonance Imaging Brain Correlates Of Deception In Healthy Young Men*, The Journal of Neuropsychiatry and Clinical Neurosciences (Volume 16), 2004, pp. 295-305.

subjects were instructed to decide either to subtract or add two numbers that had been showed to them[52]. Interestingly, on the basis of fMRI technology, experimenters were able to find (with up to 70% accuracy) whether participants would subtract the presented number from the other or whether they would sum the numbers.

Apart from these laboratory experiments, Sean Spence[53], who has pioneered the use of this groundbreaking technology, carried out a real-life experiment in 2008. He investigated the potential innocence of a woman who had been convicted of intentional inducing illness in a child (and later was sentenced to four years in prison. According to Spence, this ground breaking research proves that fMRI has the potential to reduce the number of miscarriages of justice and capacity to address the question of guilt versus innocence. According to some other researchers[54], fMRI can help you to look in a person's brain to determine if he or she has been to any specific place before, so if a person was in any terrorist training camp before, you can actually determine that. To sum up, according to this and many other studies, this technology is claimed to be useful in investing personality traits, mental illness, religious

[52] Haynes, John-Dylan, Katsuyuki Sakai, Geraint Rees, Sam Gilbert, Chris Frith and Richard E. Passingham, *Reading Hidden Intentions In The Human Brain*, Current Biology (Volume 17), 2007, pp. 323-328.

[53] Spence, Sean A., Catherine J. Kaylor-Hughes, Martin L. Brook, Sudheer T. Lankappa and Iain D. Wilkinson, *Munchausen's Syndrome By Proxy' Or A 'Miscarriage Of Justice'? An Initial Application Of Functional Neuroimaging To The Question Of Guilt Versus Innocence*, European Psychiatry (Volume 23, Issue 4), 2008, pp. 309-314.

[54] BBC, *Minds of our own?* Transcript of a recorded documentary, 2010. Available online at: http://news.bbc.co.uk/nol/shared/spl/hi/programmes/analysis/transcripts/15_03_10.txt.

extremism, racial prejudice, lie detection and employee screening.

Not only has this neuro-imaging technology taken the attention of scientific communities but it has also attracted interest of the press and corporate world[55], as outside the legal system fMRI has also critical importance in the insurance industry for detection of deception. In result, two private companies, Cephos Corp and No Lie MRI, were launched in 2006 and have begun marketing their lie detection services and offering this technology with the goal of bringing these methods to the common public in legal proceedings and security investigations[56].

E Employee Screening using fMRI: Building Trust and Improving Security

Our research is focused on functional MRI in non clinical settings, such as employee screening in critical infrastructure. Employees at critical positions need to understand that they are very important to the state's security. In the context of critical infrastructure (i.e., normally unacceptable for non-critical situations), this research is aiming at adopting extreme measures, such as employee screening for critical personnel in order to detect malicious intent activities and susceptible behaviour and other weaknesses (drug related or domestic problems and religious extremism etc.) to uncover prior criminal records, issues with character or credit problems which can help an employer assess potential risk posed by the candidate.

[55] Bayne, Timothy, *Mindreading: From Neuroimaging To The Philosophy Of Mind*, Humanities Research Showcase, Oxford, 2011.

[56] Simpson, *Functional MRI Lie Detection: Too Good To Be True?*, 2008.

Employee screening is central to such an approach. It can deal with insider threats and will help to counter the full range of threats that critical organisation may face, up to and including terrorism. The Insider Threat Study has also revealed a surprisingly high number of malicious insiders with prior criminal convictions when hired[57]. Having access to a complete employee history is an effective way of performing due diligence to protect key assets. At one hand it is beneficial for a general improvement which ultimately leads to higher productivity, better workers, increased efficiency and will provide an acceptable level of assurance for employees who have access to protectively marked critical assets and could alleviate the burden of mistrust. Furthermore, the aim of introducing this scanning technique is also deterrence from malicious activity of any kind. Indeed this approach may deter some high risk candidates with criminal/terrorist backgrounds from applying for the job, which may save money and time in the recruitment process.

F Functional MRI: Human Security and Ethical Consequences

Although above studies reported reasonably high individual accuracy rates, there are still significant legal,

[57] Randazzo, Marisa Reddy, Michelle M. Keeney, Eileen F. Kowalski, Dawn Cappelli and Andrew Moore, *Insider Threat Study: Illicit Cyber Activity In The Banking And Finance Sector*, US Secret Service and CERT Coordination Center, 2004. Available online at: http://www.cert.org/archive/pdf/bankfin 040820.pdf. See also Keeney, Michelle M., Eileen Kowalski, Dawn Cappelli, Andrew Moore, Timothy Shimeall and Stephanie Rogers, *Insider Threat Study: Computer System Sabotage In Critical Infrastructure Sectors*, US Secret Service and CERT Coordination Center, 2005. Available online at: http://www.cert.org/archive/pdf/insidercross051105.pdf.

ethical and human security concerns must be addressed prior to moving this technology to real-world application[58]. Firstly, bioethicists have for years been debating the validating and accuracy of using fMRI technology outside of a clinical setting such as civil, forensic, and security settings. According to some critics, this approach is speculative and could raise privacy debates and it is possible that this practice might be viewed as invasive and excessive by some individuals[59]. Other argues that this technology limits the person's right to scan employee thought processes without or with his consent. It also raises concerns about the confidentiality of this information as it may violate the right to one's internal mental privacy[60]. This could exacerbate already precarious circumstances and may lead to more severe insider threats if any screening practice might be viewed as excessive by employees[61].

[58] White, A.E., *The Lie Of fMRI: An Examination Of The Ethics Of A Market In Lie-Detection Using Functional Magnetic Resonance Imaging*, HEC Forum: an Interdisciplinary Journal on hospitals' ethical and legal issues (Volume 22, Issue 3), 2010, pp. 253-266.

[59] Bizzi, Emilio, Steven E. Hyman, Marcus E. Raichle, Nancy Kanwisher, Elizabeth A. Phelps, Stephen J. Morse, Walter Sinnott-Armstrong, Jed S. Rakoff and Henry T. Greely, *Using Imaging To Identify Deceit: Scientific And Ethical Questions*, American Academy of Arts and Sciences, Cambridge, 2009.

[60] Wolpe, Paul Root, Kenneth Foster and Daniel D. Langleben, *Emerging Neurotechnologies For Lie-Detection: Promises And Perils*, American Journal of Bioethics (Volume 5, Issue 2), 2005, pp. 39-49.

[61] Greitzer, Frank L. and Deborah A. Frincke, *Combining Traditional Cyber Security Audit Data With Psychosocial Data: Towards Predictive Modelling For Insider Threat Mitigation, Insider Threats In Cyber Security*, Insider Threats in Cyber Security: Advances in Information Security (Volume 49), 2010, pp. 85-113.

Secondly, many of the issues are directly relevant to the fMRI experts, their expertise and public responsibility as well as the transparency of ethic issues regarding the conduct of this neuro-imaging research[62]. Thirdly, an employee who failed an fMRI test could still assert reasonable doubt in the organisation, unlike the case with DNA identification, for instance, with which the odds of being falsely recognized are on the order of millions to one[63]. According to Heckman and Happel[64] fMRI has some significant disadvantage from a human security point of view. For instance, if the subject has a metallic objects in their body and is brought into the scanning room, it could be unsafe because of the strong magnetic field inside this machine. It is also risky for people with claustrophobia and pregnant women to go through the scanning process. Fourthly, organisations have to answer some critical questions regarding under what circumstances an agency should be allowed to look for screening with this technique[65], and finally, it remains an open question how well employee screening with fMRI technology would work to ensure that human security is considered as important as state security.

[62] Choudhury, Suparna, Saskia Kathi Nagel and Jan Slaby, *Critical Neuroscience: Linking Neuroscience And Society Through Critical Practice*, BioSocieties (Volume 4), 2009, pp. 61-77.

[63] Simpson, *Functional MRI Lie Detection: Too Good To Be True?*, 2008.

[64] Heckman, Kristen E. and Mark D. Happel, *Mechanical Detection Of Deception: A Short Review*, in: Swenson, Russell (ed.), *Educing Information: Interrogation: Science And Art-Foundations For The Future,* National Defense Intelligence College Press, Washington, D.C, 2006, pp. 63-93.

[65] Marks, Jonathan H., *Interrogational Neuroimaging In Counterterrorism: A "No-Brainer" Or A Human Rights Hazard?* American Journal of Law and Medicine (Volume 33), 2007, pp.483-500.

G Functional MRI and the Dynamics between Human and State Security

According to White (2011)[66] ethical conflicts often arise when clinical technology is used for non-clinical purposes. However, it should be clear that fMRI is not a mind reading technology[67]. According to Jones (2009)[68] this technique does not provide any precise conclusion about a person's thought or what a person is thinking. It can only show a difference across time, across location and across tasks. This technique is very good at discovering when brain tissues are active during different cognitive tasks. This strongly suggests that fMRI does not violate the right to internal mental privacy. Secondly, White (2010)[69] pointed out that fMRI is ethically acceptable in the market to the same extent as traditional polygraphs, and if clients are permitted to undergo a traditional polygraph examination in employee screening, the argument is equally strong concerning fMRI scans.

However, the human security issues raised by critics are complex and it is possible that this technology may be misused by some organisations. The challenge, therefore,

[66] White, *The Lie Of fMRI: An Examination Of The Ethics Of A Market In Lie-Detection Using Functional Magnetic Resonance Imaging*, 2010.

[67] Schweitzer, N.J., Michael J. Saks, Emily R. Murphy, Adina L. Roskies, Walter Sinnott-Armstrong and Lyn M. Gaudet, *Neuroimages As Evidence In A Mens Rea Defense: No Impact,* Psychology, Public Policy, and Law (Volume 17, Issue 3), 2011, pp. 357-393.

[68] Jones, Owen D., Joshua W. Buckholtz, Jeffrey D. Schall and Rene Marois, *Brain Imaging For Legal Thinkers: A Guide For The Perplexed*, Stanford Technology Law Review (Volume 5), 2009.

[69] White, *The Lie Of fMRI: An Examination Of The Ethics Of A Market In Lie-Detection Using Functional Magnetic Resonance Imaging*, 2010.

is to forge a consensus on balancing the pursuit of human and state security to protect critical infrastructure. Consequently our aim in this research is to find a good combination of ethical guidelines that could ultimately become a general method for employee screening in critical situations and conversely decrease the extent to which it is misused or misunderstood:

1. Informed consent should be sought before fMRI scanning as the employee should be aware of the potential dangers and he/she should read, understand and sign an informed consent disclaimer to ensure that all the necessary requirements are met.

2. fMRI scan should not be allowed and should be unconstitutional unless it is done with the informed consent of the employee[70]. An employee who undergoes an fMRI scanning process must not be harmed by incidental findings.

3. Any pre-employment screening process must be compatible with all relevant legislations, for instance, Human Rights legislation. Question should be limited to a verification of the “real” or “personal” identity such as education, employment history, court records, credentials and other data associated with an employee.

4. In post-employment screening a policy can be introduced of only screening in case of

[70] Simpson, *Functional MRI Lie Detection: Too Good To Be True?*, 2008.

suspicious activities. Drug testing policies[71] of the Österreichischer Gewerkschaftsbund (ÖGB) in Austria, Deutscher Gewerkschaftsbund (DGB) in Germany, and the Confédération Générale de Travail (CGT) in France are suitable case studies for this approach.

5. There must be greater regulatory controls in place to protect employees during fMRI scans including the required training of fMRI operators. Operators should be required to participate in training and receive certification and only trained experts are required to evaluate employees and conduct the scan. Secondly, an accrediting body should certify fMRI facilities. It must ensure that employees with metal plates or screws in their bones, pregnant women and claustrophobia patients should not be scanned[72].

6. If an expert does not detect any abnormal behaviour, the employee is not harmed. However, if an abnormality is detected, the results of the scan should be analysed by at least another highly trained expert and possibly rectified.

7. To assure the safety of the employee, the fMRI scan process should undergo a complete

[71] International Labour Office, *Ethical Issues In Workplace Drug Testing In Europe*, 2003. Available online at: http://www.alcoholdrugsandwork.eu/resources/ilo-ethical-issues-in-workplace-drug-testing-in-europe.pdf.

[72] Rosen, Allyson C. and Ruben C. Gur, *Ethical Considerations For Neuropsychologists As Functional Magnetic Imagers,* Brain and Cognition (Volume 50, Issue 3), 2002, pp. 469-481.

governmental approval process to make reasonable assurance of employee's safety.

8. Employees' rights must be protected by Article 8[73] of the European Convention on the Protection of Human Rights and Article 12[74] of the Universal Declaration of Human Rights. For instance, Article 8 guarantees the right to privacy, except "*in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder and crime, for the protection of health and morals, or for the protection of the rights and freedoms of others*".

9. fMRI scanning must ensure the privacy issue links to the question of data protection. The scan must implement the United Nations International Labour Organisation (ILO) code of practice on the Protection of Workers' Personal Data (1996)[75] as well as European Union Guidelines 95/46 and 97/66 on data protection.
10. A critical organisation that dismisses an employee for failing an fMRI scan test must be able to justify the action against him/her under the influence of a Human Rights Act such as the

[73] Council of Europe, European Convention of Human Rights, (as amended by Protocols Nos 11 and 14), 1950. Available online at: http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/ENGCONV.pdf.

[74] General Assembly of the United Nations, Universal Declaration of Human Rights, 1948. Available online at: http://www.un.org/en/documents/udhr/index.shtml#a12.

[75] International Labour Office, *Protection of Workers' personal data*, 1997. Available online at: http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf.

European Convention on Human Rights (ECHR)[76] or the UK Human Rights Act 1998[77].

11. Government should ban fMRI scanning in relation to non critical organisations and should also ban any non-research use of fMRI scan until it is approved by a regulatory agency.

H Conclusion

In this research, we examined the use of fMRI in critical infrastructure to detect insider threats and conclude that this brain imaging technology can be an important, helpful, and successful tool for maintaining state security, as it may provide a more reliable method of getting and evaluating information from individuals. Furthermore, the method of dealing with employees should start in the hiring process. A consistent practice of performing background checks and evaluating individuals based on the information (such as past employment, previous criminal convictions, drug related problem and verify credentials) obtained through fMRI can reduce insider threats in critical infrastructures. However, there are ethical and legal concerns that must be considered before employing this technique. These proactive measures should not be punitive in nature; rather, the employees should be educated about them with appropriate care. Our guidelines and research show that human security should be considered as equally important as the security of state. However, employees' working at critical positions must understand that under certain circumstances such as

[76] Council of Europe, European Convention of Human Rights, 1950.

[77] British Parliament, Human Rights Act, 1998. Available online at: http://www.legislation.gov.uk/ukpga/1998/42/contents.

terrorism threats, the security of the state takes precedence, and respect for national sovereignty must prevail, as security of the whole nation may be threatened. However, if the fMRI scanning process is fully disclosed, explained and managed equitably, it is not as likely to be considered unfair by employees in critical positions and the mutual trust relationship required for an organisation is more likely to remain intact. The fMRI scanning process then becomes a known and understood element of the conditions of employment. Furthermore, government regulation appears to be a good way to accomplish this milestone. Our research is a first step towards maximizing the benefits of this emerging technology while minimizing the harms. It is our conclusion that the use of fMRI for employee screening can be accepted under the condition of informed consent. However, the best and first line of defence is a commitment by organisations to ensure that insofar as it is possible, its employees are satisfied, engaged and treated fairly.

Cristina Pace*

Balancing Rights in the Information Society: Human Rights and the Protection of Public Security

Abstract

This contribution tries to shed some light on the specific challenges of protecting both human rights and human security in the information society. Specific challenges indeed arise when attempting to reconcile the countervailing interests of privacy, freedom and security: the protection of some basic rights, particularly relevant in our contemporary information and knowledge society, such as the right to privacy and freedom of expression, seem in some cases to be undermined in the name of public security's concerns. Such rights are analyzed in their specific interconnection with the legitimate protection of public interest and security, yet recognizing that a broader definition of this concept is needed. A particular attention is dedicated to the analysis of the use of the proportionality principle as an essential tool for adjudication, especially of constitutional rights. This analysis shows how the application of the proportionality principle is not always sufficient in order to guarantee the supremacy of human rights, yet it can still be considered as a safeguard against the indiscriminate use of legislative and administrative powers exercised by a state or a public authority. It seems essential to find adequate solutions for

* E.MA. (European Master's Degree in Human Rights and Democratization), currently a Marie Curie Research Fellow at the Institute of International Law and International Relations, University of Graz (Austria) and a PhD candidate at the Department of Philosophy of the Faculty of Human and Social Sciences, New University of Lisbon (FCSH). The author can be contacted by email at: pace.cristina@hotmail.it. The present contribution builds on a previous research, "Robert Alexy's *A Theory of Constitutional Rights* critical review: key jurisprudential and political questions" (forthcoming, Dinâmia Working Paper, available online at: http://dinamiacet.iscte-iul.pt/working-papers).

balancing human rights and human security, lowering the level of threats while preserving the rights of citizens, clearly defining what the limits and responsibilities of states and organizations are. Human rights protection should be seen as a fundamental and integral part of the concept of human security: one concept in fact does not exclude the other.

Keywords: Human Rights, Constitutional Rights, Information Society, Human Security, Public Security, Proportionality Principle, Right to Privacy, Freedom of Expression, Individual and Collective Rights, Hierarchy of Rights

A Introduction

In this paper the specific challenges of protecting both human rights and human security in the information society will be tackled from the perspective of human and constitutional rights theory and moral philosophy[1], with a particular concern to the issue of balancing conflicting rights in courts, the related use of the proportionality principle and the overall issue of defense of human rights between individual and collective interests.

Relevant examples of case law, political and legal measures adopted by courts, states and international organizations, will be taken into account, in which the issue of conflicting rights concerns the balancing of basic fundamental rights with issues of public interest and state security.

It becomes clear in constitutional and international human right law nowadays that the issue of whether there is a right which has an “absolute value” and whether this value should be balanced against concerns of public interest is not an easy one to be solved. The question of

[1] Reference will be made especially to the legal philosophy of Robert Alexy and relative critiques, and to the legal and moral philosophy of Joseph Raz and Ronald Dworkin.

whether such an inalienable core of fundamental, “non-derogable rights” exists, to which weighing and balancing should not apply because of their absolute and “deontological value”[2], is nowadays of primary importance not only for practical but also for theoretical reasons. It is especially relevant in order to define whether it exists a “hierarchy of human rights” in contemporary international law.

The indication of a right as an “absolute right” can be considered as more an exception than the rule in contemporary court’s judgments procedures. As a matter of facts, whenever a conflict of rights exists, proportionality is the principle used in order to give good reasons for interference with a fundamental human right, interference that must be however justified as appropriate, necessary and proportionate.[3] But is proportionality a truly rational methodology or is it just a pragmatic method for solving conflicts in courts? Is it really a rational, legitimate and democratic interference tool? How to address conflicts of rights if not through proportionality and balancing? Which alternatives can be found, if at all, to the balancing approach?

A second important issue concerns whether it is correct to balance subjective individual rights against policies of public interest meant to safeguard some collective goods. Although the most common fundamental right is a subjective, individual and negative right, many

[2] Deontological ethics or deontology (Greek: δέον (deon) means ‘obligation’ or ’duty’) is an approach to ethics that focuses on the rightness or wrongness of the actions themselves, as opposed to the rightness or wrongness of the consequences of those actions.

[3] Cf. Council of Europe, *The Margin Of Appreciation*, n.d., http://www.coe.int/t/dghl/cooperation/lisbonnetwork/themis/ECHR/Paper2_en.asp. (All websites used in this essay were last checked on 21 June 2012).

scholars consider that fundamental rights can embrace not only individual rights but also collective goods. A conflict is therefore possible between an individual fundamental right (such as freedom of expression) and a public policy aiming at safeguarding some collective interest (as for example in the case of public security measures). The question is: should a public, collective interest such as public security prevail on fundamental basic rights of individuals such as the right to privacy and freedom of expression? And, if so, to what extent?

The solution to this problem appears much easier in the case of “even more basic” human rights such as the fundamental right to life and human dignity, which includes, at least in Europe, the prohibition of death penalty and the prohibition of torture.[4]

However, even in those cases, the reasoning followed by courts does not seem to be always clear and coherent and even basic human rights such as the right to life and the right not to be tortured are questioned and subjected to a balancing approach. Striking governments’ violation of international human rights legal standards have been widely reported and documented by activists and international NGOs worldwide. They have been also legally challenged, as for example in the case of the extraordinary rendition, illegal detention and ill treatment of detainees, practiced by US government in the prison of Guantanamo Bay and Abu Ghraib, in the framework of the US “war on terror”. After the 9/11 attacks in New York, in 2001, the Bush administration has been accused of using torture techniques against detainees, including sleep and food deprivation, waterboarding, prolonged nudity, forced standing, long-term use of loud noises, exposure to

[4] At least as concerning Europe, the death penalty has been effectively abolished since all Member States have meanwhile ratified Protocol No 6 to the European Convention on Human Rights.

extreme cold or heat and total darkness. At Abu Ghraib, US military and CIA interrogators used forms of torture that involved lasting physical damage, sexual humiliation, and sometimes death. "*These abuses across several continents did not result from the acts of individual soldiers or intelligence agents who broke the rules: they resulted from decisions of senior US leaders to bend, ignore, or cast rules aside*".[5] Particularly worrying as well as contradictory is the recent debate in favor of the "juridification of torture". Although torture is clearly prohibited by customary international law, the practice has long been considered as justifiable and necessary in the name of public security concerns. Especially in the framework of the US "war on terror", a number of respectable politicians, scholars and lawyers have begun to present sophisticated arguments seeking to justify torture in certain circumstances, in particular to prevent acts of terror.[6]

The debate around the justification of such governments actions as a legitimate exercise of state sovereignty in name of public security concerns, is still open, highly contested and at the center of many theoretical debates. A deep contestation is concerning also the debate about governments interference with the privacy of their citizens, the more or less legitimate limitation of freedom of expression and the censorship

[5] See Human Right Watch, *Getting Away With Torture. The Bush Administration And Mistreatment Of Detainees*, at p. 4, http://www.hrw.org/reports/2011/07/12/getting-away-torture-0.

[6] Harvard Law Professor Alan Dershowitz has been for example seriously criticized for suggesting the introduction of a legal regulation of torture, stating also that torture happens anyway, regardless of international conventions. For an extended reflection on the contemporary debate about torture and terrorism please refer to: Kahn, Paul W., *Sacred Violence. Torture, Terror, and Sovereignty*, University of Michigan Press, USA, 2008.

threats advanced by both states and organizations (also with regard to information and communications technologies (ICTs), social media and networks). These are only some of the most burning contemporary issues and “ethical dilemmas” on human rights nowadays, which must be taken into consideration. What is clear is that the level of security threats should be lowered while taking into account the rights of both individuals and collectivities, clearly defining their responsibilities and what the limits and contents of rights are.

The material in this essay is divided into three main sections. The first section provides a general reflection on the relationship between human rights and human security in the information and globalized era, considering its evolution, development and reconceptualization during the last century. The second section will provide a general definition and description of the principle of proportionality and the discussions concerning its legitimacy, analyzing to what extent it results effective in protecting the rights of both individuals and collectivities. The third section will explore the concept of human rights between individual and collective interests and finally discuss some conclusions, recommendations and proposals for action.

B Human Rights and Human Security in the Information Society

The last decades have been characterized by some extensive developments and changes, which are shaping the new “global society”. After agricultural and industrial revolutions, the world is now entering a new society, which is already named “information or knowledge society”.[7]

[7] The prediction of a “global information society” can be associated with Marshall McLuhan’s theory of the world’s

The main features of the information society have been delineated in various seminars, academic writings, conferences and policy documents of governments, regional and international organizations. Frank Webster for instance provides five analytical criteria in defining the information society. These are: technological; economic; occupational; spatial and cultural.[8]

Policy makers of the G7 (now G8) group of nations recognized that:

> "*Progress in information technologies and communication is changing the way we live: how we work and do business, how we educate our children, study and do research, train ourselves, and how we are entertained. The information society is not only affecting the way people interacts but it is also requiring the traditional organizational structures to be more flexible, more participatory and more decentralized*".[9]

Information society is therefore a term for a society in which the creation, manipulation and distribution of information has become the most important economic,

transformation into a "global village" by communications and media. See McLuhan, Marshall, *Understanding Media: The Extensions Of Man*, Mentor, New York, 1964 and McLuhan, Marshall and Bruce R. Power, *The Global Village: Transformations In World Life And Media In The 21st Century*, Oxford University Press, New York, 1992.

[8] Webster, Frank, *Theories Of The Information Society*, Routledge, London, 1995, 2nd edition (2002), 3rd edition (2006).

[9] G7, Conclusions of G7 Summit "Information Society Conference", *A Shared Vision Of Human Enrichment*, DOC/95/2, Brussels, 1995. Available online at: http://europa.eu/rapid/pressReleasesAction.do?reference=DOC/95/2&format=HTML&aged=1&language=EN&guiLanguage=en.

political, social and cultural activity. The knowledge economy can furthermore be described as deriving from a combination of:

> "*four interdependent elements: the production of new knowledge, mainly through scientific research; its transmission through education and training; its dissemination through the information and telecommunications technologies such as computers, computer networks and Internet; its use in technological innovation for new industrial processes and services*".[10]

In parallel with these changes and evolution in the global society, individual states, as well as international and regional organizations, including UN, EU, the Council of Europe, OSCE and NATO, have started to elaborate a set of principles, codes and declarations in order to set up a normative framework and to establish specific rules and codes of conduct for regulating risks, benefits and new challenges in the information society. That is the reason why, for example, the G8 have started to develop its own key principles for Internet governance, as well as multi-stakeholder coalitions have been created in order to develop a set of rights and principles for Internet governance. Civil society also participated in this process by calling for its own set of principles and rules.[11] International lawyers are actually discussing the interaction of these different sets of principle and their

[10] Ziya Aktaş, Ahmet, *Information/Knowledge Society And Europe*, Proceedings of World Academy of Science, Engineering and Technology (Volume 8), 2005, pp. 1-6, at p. 1.

[11] An Internet Governance Forum (IGF) was held in Nairobi in 2011 in which basic principles for Internet governance have been established. Such principles will be further developed at the next IGF meeting which will be held in Baku in 2012.

possible translation in the language of more traditional legal obligations.

It is however important to underline that, while stressing the democratic nature and positive aspects of information society, some dangers and negative aspects should not be underestimated, first of all the increasing distance and digital divide between nations, regions, companies and people. Investigating the benefits and risks of ICTs, in 1995 and 1997, the United Nations Commission on Science and Technology for Development (UNCSTD) showed that the use of ICTs, while entailing extensive social and economic benefits, contains also a high risk that technologies and services will deepen the disadvantages of those without the skills and capabilities to make the investments required for building innovative ICT-based societies.[12] Among positive aspects of information society we can mention:

> “*universal access to information for everybody, transparency and openness in government activities, electronic democracy, improvement in education and training, betterment of employment, support of market economy, various legal and social benefits and finally research and development improvement*.”[13]

Among the major risks a:

> “*pervasive influence of IT on home, work and recreational aspects of the individuals daily routine, the stratification into new classes, those who are*

[12] Mansell, Robin and Uta Wehn (eds.), *Knowledge Societies: Information Technology For Sustainable Development*, Oxford University Press, Oxford, 1998, at p. 1.

[13] Ziya Aktaş, Ahmet, *Information/Knowledge Society And Europe*, at p. 1.

> *information-rich and those who are information-poor, the loosening of the nation state's hold on the lives of individuals and the rise of highly sophisticated criminals who can steal identities and vast sums of money through information related (cyber) crime*".[14]

This entails a legitimate responsibility and also a duty from the part of the states, which engage in the protection of the human security of their citizens. They should also strengthen their cooperation with other states, regional and international organizations for the protection of human and public security worldwide, especially concerning the fight against terrorism and other forms of organized crime (including cyberterrorism and cybercrime).

As concerning Europe, the creation of an area of freedom, security and justice by the European Union, as an objective set up by the Treaty of Amsterdam in 1997, brought developments also in the fight against terrorism. Especially as a consequence of the terrorist attacks in New York 9/11 and London in 2005, the European Commission stressed the need to maintain high priority on the prevention and fight against terrorism, generally recognizing that the fight against terrorism and other serious forms of organized crime is a shared responsibility of all member states of the European Union. The Council of Europe, on the other hand, has recently agreed to promote its co-operation with the European Union, *inter alia*, in relation to "*combating terrorism, organized crime, corruption, money laundering and other modern challenges, including those arising from the development of new technologies*."[15]

[14] Collin, Simon. M.H., *Dictionary Of Information Technology: 10,000 Terms Clearly Defined*, Peter Collin, USA, 2002 (3rd edition).

[15] Council of Europe, *Memorandum Of Understanding Between The Council Of Europe And The European Union*, 117th

European measures in the fight against terrorism and organized crime include the creation of a coherent system of criminal justice, the enhanced cooperation between member states of the European Union and intelligence services, the strengthening of law enforcement authorities such as Europol and Eurojust and the improvement of information exchange, including the processing of more personal data. Such measures taken at the European level represent an example of a worldwide effort in order to improve security: the USA have for example established the Department of Home Land Security which requires the use and processing of all air passengers data throughout the world.

Of course all these developments create a situation in which it becomes always more complicated to combine such security measures with an adequate protection of privacy and human rights of individuals. As emphasized also by the Council of Europe's Commissioner for Human Rights, Thomas Hammarberg, in his issue paper *Protecting the Right to Privacy in the Fight Against Terrorism*, "*terrorism must be fought, but not at the expense of human rights protection*" and, in the fight against terrorism and organized crime, the human rights standards and principles "*should not be abandoned but, rather, re-affirmed*".[16] The study illustrates how freedom and protection of human rights have been undermined, especially in response to the terrorist attack on 9/11, when states felt entitled or even obliged to take the most drastic action against terrorism. Even the UN Security Council, without having adopted any clear and universally agreed definition of "terrorism", "*mandates punitive actions against*

Session of the Committee of Ministers, CM(2007)74, 11 May 2007, para. 26.

[16] Council of Europe: Commissioner for Human Rights, *Protecting The Right To Privacy In The Fight Against Terrorism*, CommDH/IssuePaper(2008)3, 4 December 2008, at p. 14.

(suspected) terrorists".[17]

Governments decisions, said Commissioner Hammarberg:

> "*have undermined human rights principles with flawed arguments about improved security*"[18] and we are now rapidly becoming a "*Surveillance Society*", he continued, in which "*individuals are at risk of being targeted for being suspected 'extremists' or for being suspected of being 'opposed to our constitutional legal order', even if they have not (yet) committed any criminal (let alone terrorist) offence*".[19]

This situation even undermines security instead of guarantying it, particularly when specific measures are taken against specific groups of people, entailing discrimination against them and leading to the "*alienation of the groups in question*".[20] Such general surveillance raises serious democratic problems.

The response to these trends should be for Hammarberg, the:

> "*re-assertion of the basic principles of the Rule of Law as enshrined in particular, in the European Convention on Human Rights, and as further elaborated in the case-law of the European Court of Human Rights and the European Court of Justice, as*

[17] Council of Europe: Commissioner for Human Rights, *Protecting The Right To Privacy In The Fight Against Terrorism*, at p. 3.

[18] Council of Europe, Commissioner for Human Rights, *Counter-Terrorism Measures Must Not Violate The Right To Privacy*, 4 December 2008, Available online at: http://www.coe.int/t/commissioner/News/2008/081204counterterrorism_en.asp.

[19] Council of Europe, Commissioner for Human Rights, *Protecting The Right To Privacy In The Fight Against Terrorism*, at p. 13.

[20] Council of Europe, Commissioner for Human Rights, *Protecting the Right to Privacy in the Fight against Terrorism*, at p. 13.

> *well as in European legal instruments directly or indirectly inspired by the Convention and such case-law*".[21]

In any case, and as highlighted by the UN Secretary-General in March 2010, the strategic importance of both human security and human rights in order to provide solutions in a world that is always more increasingly interlinked, protecting rights of individuals citizens while safeguarding public security and peace for all should be stressed. To say it in the words of the UN Secretary-General:

> "*In today's increasingly interlinked world, where threats can potentially spread rapidly within and across countries, human security is a practical approach to the growing interdependence of vulnerabilities facing peoples and communities. As a result, the application of human security calls for people-centered, comprehensive, context-specific and preventive responses.*"[22]

The concept of human security, which has been discussed and debated in international organizations and academic circles since the 1994 Human Development Report, entails in fact not only a military and nation-state-oriented approach to security but also a more "humanized" conception of security.[23] Such "humanized" conception significantly diverges from the classical conception of

[21] Council of Europe, Commissioner for Human Rights, *Protecting The Right To Privacy In The Fight Against Terrorism*, at p. 13.

[22] United Nations Secretary-General, *Human Security*, Report A/64/701, 2010, para. 69, at p. 17.

[23] United Nations Development Programme (UNDP), *Human Development Report 1994*, Oxford University Press, USA, 1994.

international security which has been traditionally linked to the protection of the physical and political integrity of sovereign states; requiring the protection of internationally recognized boundaries, if necessary also through the use of military force, the prohibition of the use of force between states and the principle of non-intervention in the internal affairs of other states. State security in international law is therefore narrowly centered on the preservation of the sovereign states from all external threats, including the interference of other states. A more "humanized" conception of security entails instead the need of balancing the concept of state sovereignty with more concern for the individual and a closer interconnection with the concepts of human rights and human development. It seeks to provide the means for the establishment of a sustainable and long-term peace, eliminating the root causes of conflicts. The more "humanized" conception of security sustains adequate policies for resolving crises, mainstreaming human security in all activities, through a not unilateral but multi-stakeholder, people-centered and comprehensive approach.

Even if there is still no consensus concerning the exact definition of the term "security", the concept of human security should be understood beyond the traditional notion of state security, focusing more on issues of development and protection of human rights of individuals. Human security should not be guaranteed at the expense of human rights protection and human rights and principles should be rather encouraged and re-affirmed while protecting human security. Actually, one concept does not exclude the other and human rights protection should be seen as a fundamental and integral part of the concept of human security.

C Balancing Conflicting Rights: the Principle of Proportionality and its Legitimacy

Judges as well as legislators are often confronted with the challenge of conflicting rights, which in some cases represent a real constitutional as well as ethical dilemma. The coexistence of different European and international agreements and the plurality of sources of law contribute also to the struggling of judges when it comes to the concrete and consistent implementation of rules, and sometimes the legal reasoning behind those judicial deliberations seems lost.

The main problem is therefore how to address these conflicts of rights: if through balancing and a proportionality test or otherwise. It is therefore important to establish, through an analysis of the judicial practice of balancing, if the proportionality principle can be classified as a necessary and democratic tool for interference, or if it must be considered as a "purely pragmatic method", useful to justify any kind of judicial discretion in legal argumentation. The main scope is to establish whether the application of the principle of proportionality is sufficient in order to guarantee the supremacy of human rights over security concerns, preventing the legislator from violating human rights. It is important to understand also whether (if at all) it is possible to find an alternative to the balancing approach, and in this framework, to establish whether there is (or should be) a hierarchy of human rights in contemporary international law.

In his book, *A Theory of Constitutional Rights* (*A Theory*), legal scholar Robert Alexy makes a great effort in trying to characterize constitutional courts decisions as rational decisions, offering a well-developed structure of the concept of balancing, his central thesis being that constitutional rights are principles and not rules, and thus "optimization requirements" necessarily open to balancing. While in fact rules are for Alexy "*norms which are always either fulfilled or not*", representing "*fixed points in the field of the factually and legally possible*"; principles are "*norms which require that something be realized to the greatest extent possible given the legal and factual possibilities*"; they are "optimization requirements", which can be satisfied to varying degrees.[24]

However, many other scholars and philosophers reject such a quantitative approach, emphasizing other approaches to fundamental rights, which accentuate the moral foundation of rights, their "deontological value" (e.g. Jürgen Habermas).[25]

The main jurisprudential and philosophical issues at stake therefore concern: the definition of the concept of constitutional, human and fundamental rights; the definition of the structure and content of constitutional rights, the attempted establishment of their limits and scope.

In order to determine whether the proportionality test and the judicial practice of balancing actually correspond to a necessary and rational process, it is therefore important to ascertain whether such right exists which has a purely "deontological value" and cannot be limited in any case, even if in conflict with other rights.

On the other hand, judicial discretion, moral views and political ideologies play an important role in the judicial practice and there are still many rationality limits that leave a large margin of discretion to the judges in

[24] Alexy, Robert, *A Theory Of Constitutional Rights*, Oxford University Press, Oxford, 2002, at p. 47-48.

[25] According to Habermas a right having a "deontological value" is a right that cannot be limited in any case, even when in conflict with other fundamental rights. Habermas, Jürgen, *Between Facts And Norms*, *Contributions To A Discourse Theory Of Law And Democracy*, The MIT Press, Cambridge, 1998, at p. 258.

what concerns judicial decisions regarding fundamental rights. The question however arises if judicial discretion does not entail a corrosion of democratic governance, whenever judges act with excessive power in their function.

Whenever there is a conflict of rights in the judicial practice, proportionality is the principle used in order to justify the interference with a fundamental human right, interference that must be however explained as appropriate, necessary and proportionate.

Originally derived from the German basic law, the proportionality principle became one of the main fundamental principles developed by the jurisprudence of many European, national and international courts worldwide, as for example the European Court of Justice (ECJ) and the Inter-American Court of Human Rights (IACHR). The European Court of Human Rights (ECtHR) also regularly applies this principle for the purposes of delimiting the margin of appreciation allowed to states in applying the European Convention on Human Rights (ECHR).[26]

The principle of proportionality is considered as a safeguard against the indiscriminate use of legislative and administrative powers exercised by a state or a public authority: courts have always used it as a procedure aiming at guaranteeing the full respect of human rights by a state or public authority.[27] Judges apply this principle also in order to settle disputes of conflicting constitutional provisions and to develop a hierarchy of fundamental rights.

In particular, the principle of proportionality requires that any measure taken by a state or a public authority

[26] Council of Europe, *The Margin Of Appreciation*.

[27] Cianciardo, Juan, *The Principle Of Proportionality: Its Dimensions And Limits*, ExpressO, 2009, at p. 2. Available online at: http://works.bepress.com/juan_cianciardo/1.

that interferes with a basic human right must be appropriate, necessary and proportionate. The measure has to be appropriate (principle of suitability), in order to achieve the objective which is intended by the lawmaker, meaning that an eventual interference with one principle should contribute to the realization of another principle of equal importance; necessary (principle of necessity) in order to achieve such objective, meaning that there should be no other less severe means by which to achieve the same result; and proportionate (principle of proportionality *stricto sensu*), meaning that it must be reasonable, balancing both advantages and disadvantages.[28]

The task of the judges therefore will be the one of weighing *pros and cons*, advantages and disadvantages of the measure in question. This entails however that if the hypothetical advantages of interfering with a fundamental right are high, "*the way in which human rights may be affected is expected to be high too, and this will be still considered acceptable according to the principle of proportionality*".[29]

In Alexy's *A Theory* the proportionality principle is considered as a reasonable practice for solving conflicts between principles. Balancing has for him a rational structure formed by three elements (laws), which are considered as the core structure of balancing: the "law of balancing", the "weight formula" and the "burden of argumentation".

The "law of balancing" represents for Alexy the principle of proportionality *stricto sensu* and characterizes what is legally possible, while the "weight formula" and the

[28] Council of Europe, *The Margin Of Appreciation*. Please refer also to Möller, Kai, *Balancing And The Structure Of Constitutional Rights*, in: International Journal of Constitutional Law (Volume 5, Issue 3), 2007, pp. 453-68, at p. 455-456.

[29] Cianciardo, Juan, *The Principle Of Proportionality: Its Dimensions And Limits*, at p. 4.

“burden of argumentation” characterize what is factually possible. Alexy sustains that in case of impossibility of making rational judgments through these three stages of the law of balancing, the objections raised by Habermas would be justified. The two main objections to Alexy´s *A Theory* raised by Habermas are: the “firewall’s objection” which sustains that the “*balancing approach deprives fundamental rights of their normative power*” and the “*danger of irrational rulings*” namely a risk of irrational decision-making which “*takes places either arbitrarily or unreflectively, according to customary standards and hierarchies*”.[30]

The balancing operation becomes more difficult as much as it becomes more difficult to establish which the rational criteria for balancing are: for Alexy balancing will in fact admittedly depends not only on normative but also on factual premises. The normative premises, as for example the “abstract weight” of principles, depend on many relative factors such as the different concept of person in different legal and political systems, giving further room to judicial discretion. Such “concept of person” is not the same in every legal system but can change: in a Rawlsian legal system, for example, liberty rights are absolute rights which cannot be interfered by any act of public authority, while in a communitarian system a highest value would be given to the collective good, which will then prevail over individual freedom.

It may be said that: “*the measurement of the abstract weight of principles according to the triadic scale clearly depends on the ideology of the judge*” which “*solve*[s] *the case according to what is for him the best moral*

[30] Habermas, Jürgen, *Between Facts And Norms*, at p. 258.

argument". The problem is that "*sometimes it is not easy to know which the best moral argument is*".[31]

The factual premises, on the other hand, concern their reliability. However it is sometimes very difficult to establish the reliability of a case considered as from different perspectives: sometimes the knowledge of the judge concerning empirical facts can be very limited.

As pointed out by Carlos Bernal Pulido in his article *On Alexy's Weight Formula* the most critical point in balancing is that:

> "*it is essential to make a further distinction between relatively easy cases in balancing, in which rational judgments are possible and can reasonably established through balancing; and much harder cases which appear to be more complex and in which the premises which should be considered as objectives, are often uncertain*".[32]

This demonstrates that the reference to Alexy's "weight formula" sometimes implies a grant of discretion. Finally, we can reasonably sustain with Pulido that the balancing procedure "*should not be regarded as an algorithmic procedure which produces the right answer in all cases*."[33] Judge's discretion, moral views and political ideologies still play an important role in judicial practice.

This analysis shows that the application of the principle of proportionality is not always sufficient in order to guarantee the supremacy of certain human rights over

[31] Bernal Pulido, Carlos, *On Alexy's Weight Formula*, in: Menéndez, Agustín José and Erik Oddvar Eriksen (eds.), *Arguing Fundamental Rights*, Springer, Dordrecht, 2006, at p. 108.

[32] Bernal Pulido, Carlos, *On Alexy's Weight Formula*, at p. 106.

[33] Bernal Pulido, Carlos, *On Alexy's Weight Formula*, at p. 109.

public security concerns or other human rights and does not always prevent from violating them.

At least in some circumstances, the principle of proportionality can represent just a "formal principle", "*a mere rhetoric device, useful to justify any kind of judicial decisions*".[34]

As pointed out also by Juan Cianciardo in his article *The Principle of Proportionality: its Dimensions and Limits*:

> "*if the principle of proportionality were just a balance between the 'weight' of the right and that of the reasons that have led the legislator to decide to restrict such right, then, ultimately, that human right could lose its characteristic of impassable barrier for the state. Indeed, the invocation of a more or less convincing raison d'état could justify the sacrifice of some human rights.* […]. [A]*t best, the rights will depend on the consensus; in all cases, they will never be called victories in front of the majorities*".[35]

The central question therefore is: should we accept the proportionality of a norm and the balancing exercise even in case it seems to violate a human right instead of protecting it, even when the proportionality exercise seems to be reduced to "a mere rhetoric device"?

The risk could be the one of a "judge-made law", the supreme court becoming the final arbiter of constitutional law, including the potential use of political ideologies and personal believes and even prejudices to justify sentences, fundamental rights losing their strict "deontological character" and normative power. The principle of proportionality, nevertheless, still seems to be

[34] Bernal Pulido, Carlos, *On Alexy's Weight Formula,* at p. 101.

[35] Cianciardo, Juan, *The Principle Of Proportionality: Its Dimensions And Limits*, at p. 5.

the best safeguard against the indiscriminate use of legislative and administrative powers exercised by a state or a public authority.

D Human Rights at Stake: Between Individual and Collective Interests

Although the most common fundamental right is a subjective, individual and negative right, some scholars sustain that fundamental rights embrace not only subjective rights, but also collective goods.[36]

The list of internationally recognized human rights has not remained the same over time. As early as 1977, human rights have been classified into three generations and a debate has started to include also “fourth generation rights” which are particularly relevant in our information/knowledge society.[37] These rights, also called “communication rights”, advocate for a theory of liberation of the information and are considered as universal and essential to the full participation in society. They incorporate freedom of expression and freedom to receive, seek and impart information and knowledge.

The rights of first generation, namely civil and political rights, refer to traditional civil and political liberties typical of Western liberal democracies and deal mostly with negative rights, such as the right not to be interfered

[36] For a detailed analysis of the concept of collective rights please refer to: Jones, Peter, *Human Rights, Group Rights, And Peoples' Rights*, Human Rights Quarterly (Volume 21, Issue 1), 1999, pp. 80-107.

[37] For a history of the evolution of human rights please refer to: Council of Europe, *Compass, Manual On Human Rights Education With Young People*, 2002. Available online at: http://eycb.coe.int/compass/en/chapter_4/4_2.html. Also refer to: Donnelly, Jack, *Universal Human Rights In Theory And Practice*, Cornell University Press, Ithaca, 2003.

in private life, freedom of speech, freedom of religion, right to fair trial, freedom from torture, right to personal safety. These rights are the "classical" human rights and normally presuppose a duty of non-interference on the part of governments towards individuals. For many years, the predominant position, especially in the US and in other Western states, was that only these rights were authentic human rights, a position highly criticized by non-Western and socialist countries, because it ignores alternative conceptions of human rights.

The second-generation rights are economic, social and cultural rights, which are positive rights, such as the right to employment, education, housing and health care and the right to a decent standard of living. They require a positive and affirmative action of governments for their realization and, in contrast with first-generation rights, can refer to the well-being of entire societies, or of specific subgroups in society.

The third generation rights, also called "solidarity rights", are collective rights. These rights belong to groups of people, even if not directly associated with a "person-state" relation. Rights of this generation are, for example, the right to self-determination, the right to development, the right to peace and security, the right to a healthy environment, to intergenerational equity, to communication and humanitarian assistance. The recognition of this new category of rights is necessary in a world where extreme poverty conditions, wars and natural disasters have highly compromised respect for even basic human rights. The recognition of those rights would imply, especially for countries in the developing world, the development of the appropriate pre-conditions in which also first and second generation rights could be appropriately realized and recognized. They have emerged in correspondence with increasing globalization, changing ideas about human dignity, as a result of technological developments and also as a result of new emerging global threats.

A right to human security can also be considered in my opinion as a third generation, solidarity right, focusing not only on the state but on the individual, including in its concept a broader definition of security which include the concept of development and the protection of human rights of both individuals and collectivities in a supranational and international dimension. In a world of increasing interdependence on common issues, global threats require a common action in order to be managed.

However, one of the main characteristic of the third generation rights, which at the same time make them controversial, is the fact that it is the international community and not the state which is held responsible for safeguarding them, meaning an impossibility to guarantee accountability.

Some scholars even reject the idea that collective rights can be considered as “human” rights at all, for the fact that human rights are, by definition, held by individuals while collective rights are held by communities or even whole states. They consider that individuals must be always given priority over any interests of the society or social groups. They believe for example that an acknowledgment of collective rights could provide a justification for some repressive regimes and contribute to a negation of individual human rights in the name of collective interests.

It is therefore essential to recognize whether collective rights can be considered as fundamental rights or not. Following the libertarian conception of rights means to recognize that the only authentic rights are the ones that are capable of immediate enforcement and full justiciability: those are the rights which have the value of rules and should be guaranteed at any time without limitations and exceptions. This idea is usually associated with civil and political rights (CPR), which are also the most easily enforceable as they mostly require the state to refrain from action.

On the other hand, the term “principles” is traditionally more properly used to define economic, social and cultural rights (ESR). Even though they may have an influence on the law and decision-making process, they do not create any directly enforceable right: they are considered as not capable of specific legal determination before a court, but can just provide a basis upon which to find more specific rights which could then become directly enforceable.

Rights such as the right to housing, to education, to health, to an adequate standard of living must be respected, protected and fulfilled by the states which should take “progressive”, gradual action towards their fulfillment[38], but they are in practice not easily and not always enforceable everywhere. They depend on the adoption of social policies by the states to ensure their implementation and protection. While all states should be able in principle to comply with civil and political rights, not all states are able to provide the financial and technical resources for the full realization of affirmative obligations such as education and an adequate standard of living.

The distinction between positive and negative rights is then a distinction between “programmatic” (ESR) and “justiciable” rights (CPR).

This is the reason why many national constitutions or Bills of Rights do not even include economic and social rights, containing instead only civil and political rights, considered the only capable of specific legal determination before the courts.

[38] United Nations, *International Covenant On Economic, Social And Cultural Rights*, General Assembly Resolution 2200A (XXI), 1966, 993 UNTS 3, Part II, Article 2.1.

Liberals have therefore been:

> "*traditionally anxious to protect individuals from the tyranny of democratic authority by granting rights that can be used as 'moral trumps' against the process of majority rule, while democratic theorists always defended the application of rights in view of the realization of some common good and social objective*".[39]

In any case, assuming that individual and collective rights have to be considered on the same footing, means to assume the possibility of a conflict between an individual fundamental right and a public policy aiming at safeguarding some collective interest (e.g. freedom of expression/speech, freedom of religion, right to privacy/data protection *vs* state security). It generally entails a conflict between a classical individual right and some collective interests, an opposition between individual rights and what is defined as a common good or public policy.

If we assume that collective goods have a fundamental status we are then confronted with a conflict of rights that requires balancing and weighing the conflicting positions at stake: in this case it is not possible anymore, as the liberal tradition does, to affirm that the individual subjective right should prevail on the collective interest in any case. This is however a controversial issue, still open for discussion. A main risk here would be the one of fundamental rights losing their "absolute" and "deontological character", their priority as "moral trumps" against the process of majority rule. This is aligned to the

[39] McGregor, Joan L., *Liberalism And Democracy*, Philosophy East and West (Volume 38, Issue 3), 1988, pp. 334-346, at p. 334.

Ronald Dworkin's famous metaphor of rights as "*political trumps held by individuals*" which cannot be altered, not even by consensus. For Dworkin rights have a special normative power: the reasons which they provide are

> "*particularly powerful or weighty reasons, which override reasons of other sorts* […] *Rights give reasons to treat their holders in certain ways or permit their holders to act in certain ways, even if some social aim would be served by doing otherwise*".[40]

The author considers that there can be only very few cases of exemption which can "trump" rights.

The main concern is therefore to establish whether and how it would be possible to overcome the conflict, typical of the liberal tradition, between human rights and common good, the conception by which individual fundamental rights should always have priority over any other social concern or political objective. In order to overcome this conflict it is important to understand the two different concepts. However this is in itself problematic, because the general consensus on their meaning differs within different ideologies and cultures.

A possible solution, suggested for example by Joseph Raz, could be the adoption of a so-called interest-based theory of rights as opposed to a classic will-theory

[40] Wenar, Leif*, Rights,* in: Zalta, Edward (ed), *The Stanford Encyclopedia Of Philosophy*, Stanford University Press, Stanford, 2011, at para. 5.1. Available online at: http://plato. stanford.edu/archives/fall2011/entries/rights/. See also: Dworkin, Ronald, *Taking Rights Seriously*, Harvard University Press, USA, 1978 and Dworkin, Ronald, *Rights As Trumps,* in: Waldron, Jeremy (ed.), *Theories Of Rights*, Oxford University Press, Oxford, 1985.

of rights.[41] Will-theorists like for example Herbert Hart, believe that a right makes the right holder "*a small scale sovereign*"[42], considering that "*the function of a right is to give its holder control over another's duty*" to act in a particular way. To have a right is for a will-theorist to have the normative power "*to determine what others may and may not do, and so to exercise authority over a certain domain of affairs*".[43]

However, the will-theory of right seems to be unable to give an explanation of some rights that nevertheless exist such as the rights of "incompetents" like animals, children, or handicapped people which possess rights (for example the right not to be tortured) even though they do not exercise power over them because incapable of exerting their will and sovereignty.

An interest-based theory, on the other hand, seems to be more capacious than the will-theory, considering instead that "*the function of a right is to further the right-holder's interests*". It can therefore "*accept as rights both unwaivable rights (the possession of which may be good for their holders) and the rights of incompetents (who have interests that rights can protect)*."[44] In the specific case of a conflict between fundamental individual rights and common goods, interest-based theories can shed some light by giving a different definition of rights. Following this conception, rights are based on the interest and wellbeing of single individuals even though they are not limited to the

[41] Will-based and interest-based theories are the two main theories of the function of rights. Each one of them presents itself as capturing the understanding of "*what rights do for those who hold them*". Cf. Wenar, Leif*, Rights*, at para. 2.2.

[42] Hart, Herbert L. A., *Essays On Bentham: Studies In Jurisprudence And Political Theory*, Oxford University Press, USA, 1982, at p. 183.

[43] Wenar, Leif*, Rights*, at para. 2.2.

[44] Wenar, Leif*, Rights*, at para. 2.2.

interest of individuals alone but extend their interest to the general wellbeing of the community. Rights will be then characterized as common decisions regarding fundamental interests of individuals, which however will not be separate from concerns of collective interests and goals in a society. This was clearly illustrated by Joseph Raz in his article *Rights and Politics*:

> "*The weight given to the interests of the right-holder in determining whether his interest is protected by a right, and how extensive that protection is, reflects not only our concern for the individual, but also our concern for the public interest that will be served by protecting the interest of the right holder* […], *the right's holder's interests are only part of the justifying reason for many rights. The interests of others matter too. They matter; however, only when they are served by serving the right holder's interests, only when helping the right-holder is the proper way to help others.*"[45]

In Raz's opinion, collective interests and individual rights should co-exist in harmony and cooperate with each other: there should be no tension or conflict between them. In order to achieve a comprehensive conception of human rights it is in fact essential not to underestimate the importance of common good and its influence on values such as social justice, equality and freedom. Both individual human rights and collective interests are an essential part of the human dimension and the right held by an individual always entails a duty on others. What is important for an individual cannot be considered

[45] Raz, Joseph, *Rights And Politics*, in: Tasioulas, John (ed.), *Law, Values And Social Practices*, Aldershot, Dartmouth, 1997, at p. 89.

independently of the consequences upon other individuals in a society and the individual autonomy should promote the wellbeing of the entire society.

E Conclusions

One primary conclusion that has been reached is that even when a measure respects all proportionality's criteria, it should be nevertheless declared unacceptable and unconstitutional in case it is found in violation of a basic human right: it is in fact not possible to accept the proportionality of a norm in every case, even when it is in violation of a basic human right. It follows that a norm can be considered as proportional if and only if it does not influence or change the essential content of a human right. A norm should be considered as disproportionate and unconstitutional in case it alters the essential content of a human right or in case it lacks the sufficient justification for an eventual restriction of this right. This is the reason why it becomes fundamental to be aware of the limits, content and characteristics of human rights, analyzing first of all the degree of alteration of a right in every single case. Another important conclusion that has been reached in this analysis is the one associated with a relativistic conception of justice and law, of having fundamental individual rights balanced against collective goods, public interests and policies. It is in fact necessary to analyze and clarify not only the content and characteristics of each fundamental right, but also their relationship towards each other and towards fundamental rights "of the others", meaning the relationship between human rights and the "common good" of a community, and considering also the degree of public interest involved in every case.

The evaluation of such public interest should however be done again by referring first to the essential content of rights, in order to avoid the utilitarian risk. In a few words, the most important action that has to be taken in order to evaluate a norm is to determinate which the “inalienable” content of a right is. Therefore, only once determined the inalienable content of right, it will be possible to proceed with further analysis and consideration of collective good, public interest or policy objectives, determining the level of interference of the measure taken into account.

Judges with constitutional competence should be the ones performing this task through a faithful interpretation of the constitution and an understanding of each human right in relation to his concept and essential content. Collective interests and individual rights should coexist in harmony and cooperate with each other avoiding conflicts. Both individual human rights and collective interests should be considered as an essential part of the human dimension and each right held by an individual always entails a duty and a responsibility on others.

III The Impact of ICTs on Human Rights Protection Regimes

Mahlet Fitsum Halefom*

Human Security and Internet Governance: The Impact of Social Media and ICTs on Conflict Management and Peace Building

Abstract

Information and Communication Technologies (ICTs) have led to rising worldwide connectivity and both states and societies are being impacted by these changes. Mobile phones and Internet have provided many new possibilities and media for communication. This paper highlights the impacts of ICTs on conflict management. Although it mainly focuses on the possible positive and negative effects of ICTs on conflict management and peace building, the challenges and risks that might be encountered and the possible ways of tackling them are also discussed in detail.

Keywords: Peace Building, Conflict Management, Information and Communication Technologies (ICTs)

* European Masters Degree in Human Rights and Democratization from European Inter Universities Center, Italy and at Queen's University Belfast, United Kingdom with a background of law (LLB) from Addis Ababa University. The author has worked in different governmental and non-governmental organizations (NGOs), in different posts such as lawyer, researcher, trainer in conflict management, international, regional and sub-regional relations, human trafficking, gender and gender-based violence and migration. The author has done different research on peace and conflict, human rights and human security and has contributed a number of research projects and articles at different organizations, universities and journals.

A Introduction

Freedom of expression and access to information represents a cornerstone of democratic rights and freedoms. In its first session in 1946, before any human rights declarations or treaties had been adopted, the United Nations (UN) General Assembly adopted resolution 59(I) stating "*freedom of information is a fundamental human right ….the touchstone of all the freedoms to which the United Nations is consecrated*."[1]

Communications have evolved notably since the invention of the telegraph. Today, the use of Information and Communication Technologies (ICTs) via tools such as computers, Internet and mobile phones, brings a larger diversity of agents to the conversation in many directions such as appreciating diversities, solving problems, sharing experiences and voicing out opinions without fear.[2] In previous times the world media have struggled to develop effective communication channels to serve the people. In the ICTs era the custom of media has rapidly changed: new opportunities have arisen for greater freedom of expression, even though new threats are also emerging at the same time.

This paper is an attempt to define how ICTs and social media can be used to prevent, respond to, and recover from conflict, and bring attention to the mechanisms used in order to solve such problems. The chosen topic is especially challenging and recent and, in my opinion, not adequately reviewed by scholars and

[1] Human Rights Education Association, *Freedom Of Expression*, n.d. Available online at: www.hrea.org/index.php?doc_id=408 (All websites used in this paper were last checked on 19 June 2012).

[2] Human Rights Education Association. See also Baker, Martin and Julian Petley, *Ill Effects: The Media/Violence Debate*, second edition, Questia, London and New York, 2008, p. 30.

researchers so far. While underlining the growing importance and utility of social media, the challenges inherent to the use of these ICTs must be highlighted. On the other hand, a wrong use of social media as part of a large commercial enterprise may not promote human rights, rather having a negative impact on peace and security.

The overall goal of this paper is to explicitly consider ICTs and social media in their particular impact on peace building and conflict management rather than in its general prospect, which would be too wide.

B The Impact of ICTs and Social Media

The use of ICTs in the prevention and managing of conflicts is greatly contributing to the promotion of peace.[3] ICTs serve as a channel for information exchange and to create understanding among different groups in societies. It is evident that conflicts arise due to a lack of discussion as well as misunderstandings among conflicting parties.[4] Therefore the use of ICTs can be a path towards peace and security, embracing the participatory governance principle through user friendly, harmonized and effective management tools and mechanisms.[5] Based on that, ICTs have a great impact as they reach individuals, groups and organizations around the world. This has greatly contributed to an easier and more rapid dissemination of

[3] Biztech Africa, *Africa Notes ICT's Role in Peace and Security*, 2010. Available online at: http://www.biztechafrica.com/article/africa-notes-icts-role-peace-and-security/326/.

[4] Biztech Africa, *Africa Notes ICT's Role in Peace and Security*.

[5] Biztech Africa, *Africa Notes ICT's Role in Peace and Security*.

information, and to an increased visibility of potential and actual conflicts.[6]

In the past years, ICTs have helped significantly to improve the well-being of individuals and communities at risk. In the age of the information society, social media give a new meaning to human rights, particularly freedom of expression and information, by promoting access to knowledge, mutual understanding and ways to reveal human rights abuses and promote transparent governance.[7] In relation to peace and security, ICTs have positive impacts on peace building and conflict management. They are also crucial in the construction of resilient communities enabling to prevent conflicts.[8] Besides, ICTs can help addressing the root causes of violent conflicts by promoting mutual understanding, as they constitute an essential factor in conflict prevention and a vital tool in peacekeeping and post-conflict reconciliation.[9]

On top of that, ICTs offer ways to disclose human rights abuses, promote transparent governance, and give people living under repressive regimes access to free information to make public the injustices they suffer and

[6] Fati, O.I., *Impact Of Information And Communication Technology On Conflict Management: The Nigerian Niger-Delta Conflict In Perspective*, Staff Papers, University of Jos, 2010, at p.i. Available online at: http://cisweb1.unijos.edu.ng/handle/10485/1113.

[7] Fati, O.I., *Impact Of Information And Communication Technology On Conflict Management: The Nigerian Niger-Delta Conflict In Perspective*, at p. i.

[8] Fati, O.I., *Impact Of Information And Communication Technology On Conflict Management: The Nigerian Niger-Delta Conflict In Perspective*, at p. i.

[9] Fati, O.I., *Impact Of Information And Communication Technology On Conflict Management: The Nigerian Niger-Delta Conflict In Perspective*, at introduction.

ask for support.[10] Networks such as social media are starting to discover the different ways in which ICTs can bring people together. Through the networks it is achievable to work together with different individuals, groups and organizations for various operations that can be related to conflict management, emergency response, disaster reduction and actions for post-conflict reconstruction.[11]

Furthermore, hosting discussion forums and meetings that can provide a framework for learning, have a positive impact for networking, notably in the areas of conflict mediation, reconciliation and resolution.[12] For instance, during the fighting in Burundi, online discussion groups hosted by '*Burundinet*' and the '*Burundi Youth Council*' allowed Burundi to have different sources to discuss the situation, debate root causes, and figure out ways to move forward.[13]

However, an opportunity to build coherent communities of practice is being missed by ICTs and social media. This missed opportunity can be attributed to a lack of understanding within the communities. Despite the fact that ICTs can significantly contribute to peace

[10] Peacebuilding Initiative, *Public Information & Media Development: Public Information, Media Development & Peacebuilding Processes*, nd. Available on line at: http://peacebuildinginitiative.org/index.cfm?pageId=1838.

[11] Peacebuilding Initiative, *Public Information & Media Development: Public Information, Media Development & Peacebuilding Processes*.

[12] Peacebuilding Initiative, *Public Information & Media Development: Public Information, Media Development & Peacebuilding Processes*.

[13] Cole, Ronald "Skip" and Teresa Crawford, *Building Peace Through Information And Communications Technologies*, Idealware, 2007, at p. 1-3. Available online at: www.idealware.org/articles/building-peace-through-information-and-communications-technologies.

building and conflict management, holding a potential to be positively used in this respect, negative aspects and limitations should be equally recognized. It should be noticed for example that people living in rural areas and illiterate populations mostly do not have access to modern information and communication technologies.[14] Strategies therefore need to be put in place towards eliminating illiteracy in these societies.

Furthermore, while ICTs and social media have allowed for the creation of better communication and coordination mechanisms, they have recently equally contributed to provoking conflicts, especially through the engagement of extremist groups for their own purposes.[15]

The socio-political activism in Tunisia, namely the Tunisian revolution, also known as the “Jasmine” or “WikiLeaks’ revolution” and the Egyptian revolution of 2010-2011, were largely organized, supported and driven through the use of social media-based tools such as Facebook and Twitter.[16] Besides, the students protests in Tehran in 2009-2010, known as the “Green or Facebook revolution” and the “Red Shirt” protests in Thailand in 2010 revealed a crucial impact of ICTs in a new age of social protest.[17]

The social network Facebook, which was one of the first social media tools of its kind, was launched in 2004

[14] Fati, O.I., *Impact Of Information And Communication Technology On Conflict Management: The Nigerian Niger-Delta Conflict In Perspective*, at p. 4.

[15] Fati, O.I *Impact Of Information And Communication Technology On Conflict Management: The Nigerian Niger-Delta Conflict In Perspective*, at p. 4.

[16] Melvin, Neil and Tolkun Umaraliev, *New Social Media And Conflict In Kyrgyzstan*, SIPRI Insights on Peace and Security (Number 2011/1), 2011, at p. 1. Available online at: http://books.sipri.org/files/insight/SIPRIInsight1101.pdf.

[17] Melvin, Neil and Tolkun Umaraliev, *New Social Media And Conflict In Kyrgyzstan*, at p. 1.

and today has over 600 million users worldwide.[18] The Facebook "event" in support of the Egyptian revolution was joined by more than 80,000 people online.[19]

On the other hand, post-electoral violence and institutional fragility are still among the vital political problem in Africa.[20] For instance, following the disputed presidential elections in 2007, Kenya was thrown into post-election violence which allegedly caused the loss of more than 1200 lives and which displaced an estimated 350,000 people.[21] Likewise in May 2005 Ethiopia witnessed a similar incident which led to the death of more than 193 people and the detention of more than 40,000 people.[22] Mobile phones and Short Message Service

[18] Bohler-Muller, Narnia and Charl van der Merwe, *The Potential Of Social Media To Influence Socio-Political Change On The African Continent*, Policy Brief (Briefing 46), 2011, at p. 2. Available online at: http://www.ai.org.za/wp-content/uploads/downloads/2011/11/No-46.-The-potential-of-social-media-to-influence-socio-political-change-on-the-African-Continent.pdf.

[19] Bohler-Muller, Narnia and Charl van der Merwe, *The Potential Of Social Media To Influence Socio-Political Change On The African Continent*, at p. 2.

[20] Biegon, Japhet, *Electoral Violence And Fragility In Africa: Drawing Lessons From Kenya's Experience In The 2007/2008 Postelection Violence*, paper for a presentation at the Conference "Financial Markets, Adverse Shocks and Coping Strategies in Fragile Countries", Accra, 2009, at p. 3. Available online at: http://erd.eui.eu/media/biegon.pdf. See also Lansana Gberie, *The Price Of Protest*, Monthly Journal of Institute for Security Studies (Volume 13), 2011, at p. 6.

[21] Ajayi, Kunile, *Exploring Alternative Approaches For Managing Electoral Injustice In Africa, The Case of Breast Protests In Nigeria And The Sex Strike In Kenya*, ISS paper (number 214) 2010, at p. 2-3. Available online at: http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=120979.

[22] Ajayi, Kunile, *Exploring Alternative Approaches For Managing Electoral Injustice In Africa, The Case of Breast Protests In Nigeria And The Sex Strike In Kenya*, at p. 2-3.

(SMS) were the key technologies used by the opposition for organizing protests and coordinating its supporters in the circumstances of both countries.[23] ICTs have a vital role in preventing post-election violence, guaranteeing civil and political rights of citizens such as transparency of elections, which has started to be used in a few countries, making visible the election process through the use of these ICTs. They have also an essential role in providing distance voting service to ensure broad participation in the election.

From the occurrence of these revolutions and post-election conflicts it emerged that the use of social media tools has high potential in bringing about political and social change, enhancing opportunities for political participation and opening new spaces for active citizenship.[24]

C Why People Choose ICTs and Social Media?

People have chosen new social media for various reasons such as their low cost, their accessibility (at home, at work, through smart phones, in Internet cafes), their immediateness, and inclusiveness, in the sense that more people can be included in a dialogue using new media platforms.[25] They also require fewer skills, and can be consequently managed with less training. On the other hand, traditional media's information and its sources may actually be considered as more static and invisible

[23] Teshome, Wondwosen, *Electoral Violence In Africa: Experience From Ethiopia*, International Journal of Humanities and Social Sciences (Volume 3, Issue 2), 2009, pp. 176-201, at p. 179.

[24] Teshome, Wondwosen, *Electoral Violence In Africa: Experience From Ethiopia*, at p. 179.

[25] Galtung, Johan, *Transcend And Transform: An Introduction To Conflict Work*, Pluto, London, 2004, at p. 189.

compared to ICTs, which provide much better services. The underlying argument is that the increase of these technologies is causing rapid transformations in all areas of life; and that ICTs perform an important role in unifying cultures.[26]

Besides, the government's control over communications, which includes licensing and inspections, can be used to threaten the traditional media. This could represent another reason for preferring ICTs to the traditional media, as the control over ICTs is normally less intrusive than the control over traditional media.[27] In these conditions and as a result of the restriction to the freedom of expression through press and broadcasting legislations, companies and organizations were looking to the ICTs and especially Internet as a mean for countervailing the mainstream media and provide the population with more reliable information and analysis.[28] As a result, ICTs allowed for extensive political expression against governments and made substantial contributions to these protest actions.

D Root Causes and the Impact of ICTs of Conflicts

Conflicts start because people do not agree about an issue and the reasons can be both economic and

[26] Omotosho, Babatunde Joshua, *Youths, Technology And Violent Conflicts In Africa*: *A Serious Issue Demanding Attention From African Union*, to be published, at p. 7.

[27] Valk, John-Harmen, Ahmed T. Rashid, and Laurent Elder, *Using Mobile Phones To Improve Educational Outcomes: An Analysis Of Evidence From Asia*, Pan Asia Networking, IDRC, Canada, 2010, at p. 6-7.

[28] Melvin, Neil and Tolkun Umaraliev, *New Social Media And Conflict In Kyrgyzstan*, at p. 2.

political.[29] In many circumstances, root causes of conflicts are reflected in the diversity and complexity of issues which include for example border conflict, religious views, natural resources, ethnicity or race and migration issues.

The reasons behind the popular uprising that started in North Africa and disseminated to the rest of the Arab world were essentially related to questions of equality, corruption, justice and human rights.[30] The use of social media such as Internet and mobile phones enabled the "silent majority" (silent either by oppression or lack of good governance)[31] to stand for their rights.

In Egypt social marginalization can be considered as a root cause of conflicts illustrated by the fact that, while around 150,000 businessmen and their families lived in exclusive resorts around Cairo, millions of people lived in 1500 slums.[32] In the case of Tunisia, protests came from social demands for employment, and soon were extended also to political demands. In addition the Tunisian people

[29] Mesfin, Berouk, *The Horn Of Africa Security Complex*, in: Sharamo, Roba and Berouk Mesfin (eds.), *Regional Security in the Post-Cold War horn of Africa*, Institute for Security Studies, Monograph 178, Addis Ababa, 2011, at p. 11-14. Available online at: http://www.iss.co.za/uploads/Monograph178.pdf.

[30] Louw-Vaudran, Liesl, *Revolution In North Africa: What Is Next?,* Monthly Journal of Institute for Security Studies,(volume 12), 2011, at pp. 8-10.

[31] International Security Studies, *Conference Report On A Critical Look At The 2011 North African Revolutions And Their Implications*, ISS Conference on the 2011 North African Revolutions, 2011, pp. 1-12, at p. 2. Available online at: http://www.iss.co.za/uploads/31MayReport.pdf.

[32] International Security Studies, *Conference Report On A Critical Look At The 2011 North African Revolutions And Their Implications*, at p. 8.

[33] International Security Studies, *Conference Report On A Critical Look At The 2011 North African Revolutions And Their Implications*, at p. 3.

suffered from social injustice, restrictions on freedom of speech and lack of political freedom.[33]

The protests in Egypt and Tunisia show that also unemployment can be considered as a considerable root cause of conflict. Internet usage in 2009 was slanted heavily towards younger generations, consulting Internet and using mobile technologies for extended periods of time because of their unemployment's condition. In Tunisia the high unemployment rate, especially among young university graduates, made their lives and their families' difficult. Gradually people became frustrated as the government of Tunisia failed to reduce unemployment rate. The numbers of unemployed people increased up to 700,000 in 2009 including 170, 000 students graduating from university and was expected to increase in the following year.[34]

As a consequence of unemployment, people were unable to cope with the rapid increment of food price. Food security has been challenged with the rise in food prices began in early 2007. Social insecurity together with the unaffordability of the food price resulted in the life threatening of people living in North Africa. Consequently, people were discussing on Facebook about the issue, believing in a possible change of the situation.[35] People were aware of the fact that, if the government could not

[34] International Security Studies, *Conference Report On A Critical Look At The 2011 North African Revolutions And Their Implications*, at p. 4.

[35] International Security Studies, *Conference Report On A Critical Look At The 2011 North African Revolutions And Their Implications*, at p. 2. See also Brown, Lester R., *Root Causes Of Arab Uprisings,* adapted from Chapters 7 & 11 in: *World On The Edge*: *How To Prevent Environmental And Economic Collapse*, W.W. Norton &Company, New York, 2011. Available online at: http://www.populationpress.org/publication/2011-2-brown.html.

solve the problem within a reasonable time-frame, a conflict would have occurred.

Indeed the young generation benefited a lot from the use of ICTs thanks to an increasing access to information, freedom of expression and dissemination of information. At the same time ICTs contributed to the promotion of peace, being the most obvious instrument among people using it on a daily basis.[36] In the year 2011 alone, however, United Nations reported that 6.1 per cent of the total world's population, equivalent to 203.3 million people is unemployed and that 152 million people's income is 1.15 dollar per day.[37] This means that there is still a huge potential for conflict arising as it has been shown in the cases of Egypt and Tunisia and that the dissemination of inaccurate or misleading information among people on the Internet can easily lead to the arising of conflicts. The ICTs and social media's users, in fact, especially the young generations, do not usually put too much attention about the accuracy of the information provided and are not always concerned about verifying it.

E Risks and Challenges Associated with ICTs and Social Media

Even though social media are critically important and encompass great potential for democratic dialogue, a number of risks and challenges must be identified. First of all, it is important to recognize that not everyone is

[36] International Security Studies, *Conference Report On A Critical Look At The 2011 North African Revolutions And Their Implications*, at p. 2.

[37] UN News Center, *Record Highs In Global Unemployment Likely To Persist In 2011*, 2011. Available online at: http://www.un.org/apps/news/story.asp?NewsID=37370&Cr=unemployment&Cr1.

ethically guided or rights-oriented. Thus, though new media can be a source for good, they can also be a source of evil. The Internet is the biggest tool for expression and information-sharing in the world but can also be used for instance as a platform for extreme right-wing groups, even though the international and regional instruments such as Article 20 sub-article 2 of the International Convention on Civil and Political Rights (*ICCPR),* Article 4 of the International Convention on the Elimination of All Forms of Racial Discrimination (I*CERD)* and the United Nations Human Rights Committee General Comment No. 34 on the ICCPR article 19 and 20 strictly prohibit the use of any means to promote hate speech and incite to violence. Likewise, the African Charter on Human and Peoples' Rights Article 9 and Article 28 prohibits hate speech. This leads us to another question concerning the regulation and limits of the new media, which can apparently have a potential for conflict and can be also used as a threat to international peace and security.[38]

The other significant concern is the difficulty of ensuring the reliability and accountability of facts and information disseminated through the Internet. [39] "Facts" are usually circulated with proposed actions, as we have seen in the Arab uprising. The social media users often do not give attention to the accuracy of the information and are not interested in verifying or contextualizing the information provided.[40] This lack of accuracy and/or false information in the Internet could lead to the promotion of

[39] Streltsov, A., *International Information Security: Description And Legal Aspects*, Disarmament Forum (Number 3), 2007, pp. 5-14, at p. 7.

[40] Melvin, Neil and Tolkun Umaraliev, *New Social Media And Conflict In Kyrgyzstan*, at p. 15.

conflicts.[41] Inaccurate or misleading information can have serious consequences on conflict's arising and even basic issues concerning the quality of information can make people feel that sharing information will entail a risk for their own credibility and security.[42] On the contrary, traditional media require higher standards and sense of responsibility for the accuracy of the information provided. Information through the Internet lies on the commercial companies' personal abilities and ethics responsibility and are often not accountable for consequences and consumer's reactions.[43]

Another problem arises from the unstructured nature of the Internet, which is difficult to regulate.[44] In fact regulating new media is more difficult than regulating traditional media. Besides Internet and other social media networks are not "human rights platforms", they are rather collectively part of a "business-dominated platform".[45] In any case, media, whether new or old, represent a big business. Business companies' priority concern is their own profit and commercial interest to ensure the maximum economic benefit and not the respect of international norms and standards of human rights. They are therefore likely to offer whatever the market demands, as far as that

[41] Melvin, Neil and Tolkun Umaraliev, *New Social Media And Conflict In Kyrgyzstan*, at p. 15.

[42] United Nations Information and Communication Technologies Task Force, *The Impact Of Social Media On Peace*, The United Nations, New York, 2005, at p. 25.

[43] United Nations Information and Communication Technologies Task Force, *The Impact Of Social Media On Peace*, at p. 25.

[44] Howard, Ross, *Media And Peacebuilding: Mapping The Possibilities*; Hellmich, Phil Bob, *A New Generation For Peace*, Activate The Quarterly Journal of IMPACS, 2001, at pp. 12-14.

[45] Howard, Ross, *Media And Peacebuilding: Mapping The Possibilities*; Hellmich, Phil Bob, at pp. 12-14.

supply of service is not limited by the legal frameworks in which they are operating.[46]

On the other hand, state regulations and self-regulatory mechanisms are among the measures taken for regulating Internet and the new media online. Google and Facebook have been for instance removed from some Indian domain's websites following an Indian court decision. The rationale behind this decision entails that the governments should take the necessary measures, as the court has done in this case, as *"the companies did not take steps to protect religious sensibilities*".[47]

Apart from that there is also a problem concerning the feasibility of early-warning mechanism through ICTs and social media.[48] Early-warning is a system, not a technology. The identification, detection and risk assessment of a conflict, the accurate identification of the vulnerability of a population at risk and finally the communication of information to the vulnerable population about the threat in sufficient time and clarity, constitute the system of public warning. Warning allows people to act in order to prevent conflict. Predictions of conflict based on inadequate theoretical constructs and formal models cannot capture the unique circumstances on the ground in a given region. It is ideally difficult and potentially

[46] Howard, Ross, *Media And Peacebuilding: Mapping The Possibilities*; Hellmich, Phil Bob, *A New Generation For Peace*, at p. 12.

[47] Howard, Ross*, Media And Peacebuilding: Mapping The Possibilities;* Hellmich, Phil Bob, *A New Generation For Peace,* at p. 14.

[48] Africa-EU Partnership on Democratic Governance and Human Rights, Report on the first African-EU working group meeting on freedom of expression, 2011, at p. 8. See also Sabadello, Markus, *Scenarios: ICTs For Peace And Conflict In 2020*, Project Danube, 2001, at pp. 4-5. Available online at: http://projectdanube.org/publications/.

dangerous as frequently altering the dynamics of conflict.[49] The modeling frameworks need to be enlarged in order to deal with the complex feature of conflict.

On the other hand, given the important role that ICTs have played in several popular uprisings, states have tried to limit their potential, using them for their own purposes such as propaganda and observation.[50] On top of that, both governments and the international community have made no clear attempt so far in order to activate basic conflict prevention mechanisms and have remained silent as concerning the threat of new platforms such as social media.[51]

F Conclusion

This paper addressed how communication is a fundamental social process in order to move forward access to information and freedom of expression.[52] On the other hand, it discussed the current situation of ICTs and of their impact on peace building and conflict management, addressing the risks and challenges of ICTs and social media with a particular reference to the situation of conflict in North Africa. The paper tried to explain that though every technology can be used for good or evil, no technology is a magic remedy for human problems. Understanding the potential and proper use of

[49] PCWorld, *Google Agrees To Court Order In India To Remove Content*, 6 February 2012. Available online at: http://www.pcworld.in/news/google-agrees-court-order-india-remove-content-62052012.

[50] Sabadello, Markus, *Scenarios: ICTs For Peace And Conflict In 2020*, at p. 4.

[51] Sabadello, Markus, *Scenarios: ICTs For Peace And Conflict In 2020*, at p. 32.

[52] Sabadello, Markus, *Scenarios: ICTs For Peace And Conflict In 2020*, at p. 4.

technologies can however allow us to work on peace and security more effectively.

It was also discussed how the Tunisian and Egyptian revolutions have used ICTs as a powerful tool for self-organization as well as for political outreach. The North African scenarios illustrate the potential future evolutionary paths of ICTs and their consequences for peace and conflict in the world. ICTs and social media have positive and negative aspects embodied in them. What is almost certain however is that at least some aspects and ideas from the occurrence will be observed in the future. For example, it is likely that Facebook will expand its role as a main information provider on the Internet. It is also likely that countries in the world that currently have no access or limited access to the Internet will increasingly have access. Consequently there are today voices calling for a strong legislation and security on the ICTs, particularly as concerning Internet's regulations, in order to counter real or perceived threats.[53]

However, this does not mean that the traditional media and other method of peace building and conflict management are not important. The combination of traditional media, ICTs and social media would undoubtedly obtain reasonable results.

As it has been shown throughout history, information is a key factor in conflicts around the world. However, the use of ICTs to promote conflict has received far more attention than ICTs' use to promote peace.[54] Once violence has erupted, it can be difficult to get people to focus on dialogue and mutual understanding.

[53] Sabadello, Markus, *Scenarios: ICTs For Peace And Conflict In 2020*, at p. 5.

[54] PCF World Forum, *6th PCF World Summit: Environmental Footprinting In Europe And Beyond: How Will It Shape The Corporate Agenda?, 2011.* Available online at: http://www.ecoeco.org/content/2011/08/6th-pcf-world-summit.

Nevertheless, information operations intended to promote reconciliation are relevant in all stages of the conflict cycle.[55] Therefore, prevention measures such as providing ethically guided information, promoting international and regional instruments, ensuring the reliability and accountability of facts and information disseminated through the Internet, and working on awareness rising, can have a positive impact in terms of prevention, before the conflict blows up.

In relation to preventing the use of ICTs for purposes that are inconsistent with the objectives of maintaining international stability and security, the information society should prevent the circulation of information that incite to violence and hate speech.[56] People should also be aware of the consequences of spreading wrong or false information through the Internet and thus be encouraged to avoid such an action. Freedom of expression is in fact not an absolute right and therefore may be regulated. On the other hand, regulation of freedom of expression must be done within the limitations and scope recognized under international human rights law.

Greater and closer attention needs to be paid to the new media in order to regulate how private companies could work together taking the states responsibility and legitimate regulation of new media into account. There should be an increased focus on ensuring peace and security to states.[57] Basically, governments should identify strategies to engage with private companies through

[55] The MIT Program on Human Rights & Justice, *Human Rights and Technology*, Conference Report, 2004, at p.16. Available online at: http://mit.edu/phrj/publications_phrj/PHRJ_2004_Conference_Report.pdf.

[56] The MIT Program on Human Rights & Justice, *Human Rights And Technology,* at p. 16.

[57] The MIT Program on Human Rights & Justice, *Human Rights And Technology,* at p. 16.

opportunities such as consultative workshops to which commercial actors can actively participate.[58] That would help to develop an ethical framework, which could be used to guide the commercial media sector in their work. In order to appropriately prevent the negative impact of ICTs and social media, such ethical framework is needed for a responsible use of new media and to regulate the content of social media. Guidelines should be provided in order to technically and practically regulate new media and ICTs developers (the commercial companies) should be encouraged to develop peaceful communications tools and applications on this regard.

As previously discussed, the regulation of social and new media is more difficult than that of traditional forms of media; hence the regulation mechanisms should be consistent with international law, public interest, and the promotion of peace and security.[59] These objectives can be realized first of all by conducting a research to identify and to show the magnitude of the problem, in order to find possible solutions.

Likewise, the impact of conflict on overall development has to be analyzed so that the state can provide the necessary facilities required to pay more attention and resources for effective management of ICTs, to reduce unemployment rate and food security as a world priority and to work more on democracy and human rights.

It is likely however that the political discourse on how ICTs should be governed and how ICTs can contribute to peace and security will continue in the future.

[58] Pryce, Michael C., *Mass Atrocity Response Operations: An Annoted Planning Framework*, African Security Review (Volume 18, Issue 4), 2009, pp. 81-94, at p. 82.

[59] Pryce, Michael C., *Mass Atrocity Response Operations: An Annoted Planning Framework*, at p. 82.

Maria Eduarda Gonçalves and Inês Andrade Jesus[*]

Security and Personal Data Protection in the European Union: Challenging Trends from a Human Rights' Perspective

Abstract

The protection of personal data was first addressed in the European Community by Directive 95/46/CE. This Directive sought to reconcile personal data protection with the free movement of information in the Internal Market. The processing of personal data in the areas of security policy and police and judicial cooperation was excluded from the Directive's scope of application. However, in recent times, furthered by the "war on terror", security policies have been reinforced in the European Union (EU), a key feature of these policies being the increased collection, use and exchange of information about individuals. Major electronic databases were set up. Additional measures such as the Data Retention Directive and agreements with the USA on Passenger Name Records (PNR) have also raised concerns about their bearing on fundamental rights and liberties. Remarkably though, the legal framework for the protection of personal data in the field of security is still recognisably unsatisfactory. This gap is currently in the process of being filled by way of legislative initiatives of the European Commission, submitted in January 2012.

[*] The authors are members of the Centre for Socioeconomic and Territorial Studies (DINAMIA'CET) ISCTE – Lisbon University Institute; mebg@iscte.pt, ioajs@iscte.pt. This article has been prepared as part of a research project, "Protecting privacy and personal data in a post-Charter Europe" (2011/2013), funded by the Foundation for Science and Technology, Portugal. This project is being carried out under a partnership between DINÂMIA'CET and the Faculty of Law of the New University of Lisbon (CEDIS – Research Centre for Law and Society).

Nevertheless the question remains, how the balancing between security and the right to personal data protection is being construed by the EU. This issue was rendered more acute following the upgrading of personal data protection to the status of a fundamental right by the EU Charter of Fundamental Rights. In this paper, we will seek to address this topic based on a critical consideration of the evolution and current state of legal protection of personal data in the EU.

Keywords: Security, Data Protection, European Union, Fundamental Rights, Balancing Rights

A Introduction

In recent times the world has witnessed dramatic changes in the ways data about individuals and individuals' life are accessed, processed and exchanged. Personal data are a major asset of the information economy. The amount and variety of personal information in public administrations' electronic databases are also escalating, including for law enforcement purposes. Despite the growing penchant of individuals to public exposure in social media, perhaps denoting a new perception of privacy, people are increasingly aware of the risks associated with massive collection, storage and exchange of personal data. Potential threats range from identity theft to discrimination, unwanted marketing to feelings of fear and distrust in institutions. Hence the legal protection of personal data became a key issue in the networked economy and society, ultimately a condition for human security in the contemporary world.

In this context, different interests and values conflict and clash, particularly those of public and private organisations in the more efficient handling of their services and activities by the means of data computerisation and exchange, as unrestricted as possible; and those of individuals toward the safeguard of their personal data and, ultimately, their privacy and intimacy. In the EU this tension was first addressed by Directive 95/46/EC on the Protection of Individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive).[1]

This Directive was adopted under the Internal Market provisions of European law. The processing of personal data in the areas of the common foreign and security policy and police and judicial cooperation, as well as public security, defense, state security and criminal law has been explicitly excluded from the Data Protection Directive's scope of application.[2]

Thereinafter, under the Area of Freedom, Security and Justice launched by the Treaty of Amsterdam in 1997, and of so-called "war on terror", EU security policies were progressively tightened; a central feature of these policies being the increased collection, use and exchange of information. Major databases containing data on individuals were set up, raising concerns about their bearing on fundamental rights. Remarkably though, the potential conflict between the requirements of EU internal and external security policies, on the one hand, and the protection of personal data, on the other hand, still lacks a legal basis equivalent to Directive 95/46/EC. This gap is currently in the process of being filled by way of legislative initiatives of the European Commission (Commission), submitted in January 2012.

Nevertheless the question remains, how the balancing between security and the right to personal data protection is being construed by the EU. This issue was

[1] European Parliament and the Council, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995. http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

[2] European Parliament and the Council, Directive 95/46/EC, Article 3.

rendered more acute following the upgrading of personal data protection to the status of a fundamental human right in the EU Charter of Fundamental Rights. In this paper, we will seek to address this topic based on a critical consideration of the evolution and current state of legal protection of personal data in the EU.

We will start by reviewing and comparing major trends in data protection regimes in the EU, particularly in the Internal Market and in the Area of Freedom, Security and Justice. We will then discuss the EU institutions' tendency to present stronger security measures, including reinforced information systems, on the one hand, and civil liberties and rights, on the other hand, as mutually reinforcing; and in this way undermining the truly detrimental impact on human rights of the increasing use of personal data for security purposes.

Bearing in mind that the right to the protection of personal data has been raised recently to the status of a fundamental right in the EU, we will inquire whether this development appears to matter, in the end, for duly protecting individuals.

Considering the contents of the latest proposals of the Commission for reforming the EU data protection regimes, we conclude that the adoption of the fundamental right to personal data protection has not been by itself sufficient to assure a data protection regime that resists a great deal of criticism.

B From the Internal Market to the Area of Freedom, Security and Justice: Trends in Data Protection Regimes in the EU

Data protection regimes, like the Data Protection Directive, generally rely on certain basic principles to be observed by the data controllers and processors. In particular these are: purpose limitation – personal data may only be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes; consent of the data subject to personal data relating to him being processed; data minimization – processing of personal data must be restricted to the minimum amount necessary; proportionality – personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected; and control – supervision of processing must be ensured by member states' authorities. Also, the data subjects are assigned a set of procedural rights, enabling them to consent, to have access, and to know what information about them is registered in databases, to rectify the data, and to object to data processing in certain situations. Moreover, the Data Protection Directive prohibits transfer of personal data to third countries unless the latter provide an adequate level of data protection as determined by the Commission, or unless one of the enumerated exceptions applies. In this way, the Data Protection Directive sought to reconcile personal data protection, regarded as a minimum level of protection throughout the European Community, with the free movement of information in the interest of the internal market economy.

Actually, the Data Protection Directive represents a change in the balancing of the rights of the individual vis-à-vis the interests of data controllers and processors if compared with its predecessor, the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, of 1981 (Convention 108). Indeed, the Data Protection Directive contains a catalogue of exceptions, not found in Convention 108, to the data protection principles. That is in particular the principle of consent of the individual for their personal data to be collected and processed, admitting implicit consent in defined circumstances (Article 7). Still, the Data Protection Directive has been commonly regarded as a balanced, adequate framework, duly followed by effective supervising work by data protection authorities across Europe. Paul De Hert and Vagelis Papakonstantinou maintain, "*in practice, the Directive has by now become the international data protection metric against which data protection adequacy is measured*"[3].

This Directive 95/46/EC was adopted under the Internal Market provisions of the Treaty. The processing of personal data in the areas of the common foreign and security policy and police and judicial cooperation, as well as public security, defense, state security and criminal law has been explicitly excluded from the Data Protection Directive's scope of application, at a time when these areas remained under member states' jurisdiction.[4] However, from the nineties onwards, the launching of the EU Area of Freedom, Security and Justice and the subsequent reinforcement of EU policies against crime and terror that followed the terrorist attacks of New York 2001, Madrid 2004, and London 2005, entailed growing investment in information systems as well as in police cooperation and border control. As a result, new computerized databases containing personal data were set up, namely Eurodac and VIS, demanding an appropriate legal framework. Eurodac, a database for

[3] De Hert, Paul and Vagelis Papakonstantinou, *The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System For The Protection Of Individuals*, Computer Law & Security Review (Volume 28), 2012, pp. 130-142, at p. 131. See also Hijmans, Hielke and Alfonso Scirocco, *Shortcomings In EU Data Protection In The Third And The Second Pillars. Can The Lisbon Treaty Be Expected To Help?*, Common Market Law Review (Volume 46), 2009, pp. 1485-1525, at p. 1489.

[4] European Parliament and the Council, Directive 95/46/EC, Article 3.

comparing fingerprints of asylum seekers, and VIS, the Visa Information System, were established in 2000 and 2008, and entered into operation in 2003 and 2011, respectively. These systems complemented SIS, the Schengen Information System, established in 1990, and into force since 1995. But, despite widespread concerns with the potentially adverse effects of these developments on fundamental rights, Council Framework Decision 2008/977/JHA[5] has been and remains today the unique broad legal basis for the protection of personal data in the framework of police and judicial cooperation in criminal matters, and one that has been generally acknowledged as unsatisfactory both formally and substantially.

First of all, Council Framework Decision 2008/977/JHA only applies to personal data processed in the framework of European police and judicial cooperation, leaving apart data processing at the member states level. Besides, despite the Decision’s accent on the need to “*fully respecting fundamental rights of individuals*” (Preamble paragraph 5), data protection is limited by a substantial amount of exceptions to the data protection principles and rights. An example concerns the purpose limitation principle. According to Article 11 Council Framework Decision 2008/977/JHA, personal data may be processed for other purposes than those for which they were transmitted or made available for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; for the prevention of an immediate and serious threat to public security; or any other purpose, with the prior consent of the transmitting member state *or* the consent of the data subject. An

[5] Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, 27 November 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:EN:PDF.

additional exception is admitted to the principle of data subjects' consent, in the name of the efficiency of law enforcement's cooperation *"where the nature of a threat to the public security of a member state or a third state is so immediate as to render it impossible to obtain prior consent in good time*". In this case, "*the competent authority should be able to transfer the relevant personal data to the third state concerned without such prior consent*" (Preamble paragraph 25). Though the principles of lawfulness, proportionality and purpose are explicitly affirmed (Article 3, N° 1), "*further processing* for another purpose*shall be permitted in so far as: (a) it is not incompatible with the purposes for which the data were collected; (b) the competent authorities are authorized to process such data for such other purpose in accordance with the applicable legal provisions; and (c) processing is necessary and proportionate to that other purpose*" (Article 3, N° 2).[6] Moreover, "*appropriate time limits" shall be established for erasure and review of the need for the storage of the data*" (Article 5).

A considerable margin of discretion is therefore left to the competent authorities to define the scope of the exceptions to the data protection principles and the obligations of the data controllers, as well as the meaning of what are "appropriate" time limits of storage.

At the end of the day, the main principle guiding the exchange of personal data among police and judicial authorities is "the principle of availability of information" meaning that authorities responsible for internal security in one member state or Europol officials who need information to perform their duties should obtain it from another member state if it is accessible there.[7]

[6] Emphasis added.

[7] European Commission, Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in

Remarkably, the Commission itself acknowledged the shortcomings of this regime:

"*The processing of data by police and judicial authorities in criminal matters is currently principally covered by Framework Decision 2008/977/JHA, which pre-dates the entry into force of the Lisbon Treaty. The Commission has no powers to enforce its rules, as it is a Framework Decision, and this has contributed to uneven implementation. In addition, the scope of the Framework Decision is limited to cross-border processing*."[8]

Likewise, in its 2010 Communication "A comprehensive approach on personal data protection in the European Union", the Commission conceded, Framework Decision 2008/977/JHA contains too wide an exception on the purpose limitation principle.[9] The Commission further admitted that this and other weaknesses may directly affect the possibilities for individuals to exercise their data protection rights, e. g. to know what personal data are processed and exchanged

the area of JHA, COM (2005), 597 final, 24 November 2005, at p. 3, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0597:FIN:EN:PDF.

[8] European Commission, Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century*, COM (2012) 9 final, 25 January 2012, at p. 9. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF.

[9] European Commission, Communication on *A comprehensive approach to the protection of personal data in the European Union*, COM (2010) 609 final. 2010. Available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF.

about them, by whom and for what purpose, and on how to exercise their rights.[10]

Such a recognizably insufficient scenario from the standpoint of the safeguard of personal data used for security purposes is made more serious in view of other legislative measures taken by the EU in recent years prompting even larger apprehension with EU "securitarian trends", particularly:

a. The adoption, under pressure from USA's authorities following 9/11, of Council Regulation (EC) Nº 2252/2004 on standards for security features and biometrics in passports and travel documents issued by member states, amended in 2009.[11] The "biometric passport" has raised concern for its bearing on people's intimate features as well as autonomy since with biometrics the human body is being modeled and digitalized and turned into an instrument under control.

b. The successive PNR agreements with the USA obliging European air travel companies to transmit to Homeland Security authorities in the US several data about individuals travelling to this country.[12]

[10] European Commission, COM (2010) 609 final, at p. 14.

[11] European Parliament and the Council, Regulation (EC) Nº 444/2009, amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by member states, 28 May 2009. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:142:0001:0004:EN:PDF.

[12] Council of the European Union (EU), Council Decision 2007/551/CFSP/JHA on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of

This agreement is in the process of being revoked and replaced by another just approved by the Civil Liberties Committee of the European Parliament (March 2012). Back in December 2011, the European Data Protection Supervisor (EDPS) considered that: "*Any legitimate agreement providing for the massive transfer of passengers' personal data to third countries must fulfil strict conditions. Unfortunately, many concerns expressed by the EDPS and the member states' data protection authorities have not been met*."

c. Directive 2006/24/EC (Data Retention Directive) imposing strengthened obligations on telecommunications operators to collect and store data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.[13]

Directive 2006/24/EC aimed to harmonize rules on data retention across member states in order to ensure the availability of traffic data for anti-terrorism purposes, in case of investigation, detection and prosecution of this crime. Operators are obliged to retain a wide range of data

Homeland Security (DHS) (2007 PNR Agreement), 23 July 2007. Available online at: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/l_204/l_20420070804en00160017.pdf.

[13] European Parliament and the Council, Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 15 March 2006. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

between 6 and 24 months from the date of communication, and provide to the competent national authorities without undue delay, if requested, incoming and outgoing phone numbers fixed and mobile, the duration of phone calls, IP address, log-in and log-off times and e-mail activity details. In fact, the Directive is an illustration of a wider trend, also manifested in the PNR agreements, to preventively store personal data of all costumers. Unsurprisingly, to the question: "*What should we expect from the future?*" Stefano Rodotà answered "*there are reasons for pessimism*". And, the author adds, "*The fundamental right to data protection is continuously eroded or downright overridden by alleging the prevailing interests of security and market logic*."[14].

Personal data are more and more recorded, exchanged and retrieved at a European scale involving police and security systems as well as private entities such as telecommunications operators and aircraft companies. Not only is there more information available about individuals, but new techniques are also being developed to use data and information in increasingly sophisticated ways. Searching techniques such as data mining allowing information to be collected amid huge amounts of data, and methods for assessing risk of specific individuals based on profiling associated with stereotypes like race and religion are increasingly being employed.[15]

[14] Rodotà, Stefano, *Data Protection As Fundamental Right*, in: Gutwirth, Serge, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds.), *Reinventing Data Protection*, Springer, The Netherlands, 2009, at p. 77 and p. 80.

[15] Hijmans and Scirocco, *Shortcomings In EU Data Protection In The Third And The Second Pillars. Can The Lisbon Treaty Be Expected To Help?*, at p. 1491.

C Balancing Security and the Rights to Data Protection and to Privacy

One might notice that, notwithstanding the wide recognition of the strains imposed by EU security policies upon data protection principles and rights, EU institutions' discourse has often taken a conciliatory stance. It appears to presume that stronger security measures, including reinforced information systems, on the one hand, and civil liberties and rights, on the other hand, can be easily well-adjusted.[16] This view has been underlined in several EU policy documents: instead of a "zero sum game", the official description points to a "win-win" situation.[17] The argument has been built around the idea that security measures can be instrumental in guaranteeing privacy (e. g. when employed to control access through fingerprint or other recognition technique), countering the idea of "more security, less privacy".[18]

Decision No. 1982/2006/EC of 18 December 2006 approving the 7th Framework Programme on Research

[16] Goold, Ben and Liora Lazarus, *Introduction: Security And Human Rights*, in: Goold, Ben and Liora Lazarus (eds.), *Security And Human Rights*, Hart Publishing, Oxford, 2007, pp. 1-24. See also Liberatore, Angela, *Balancing Security And Democracy, And The Role Of Expertise: Biometrics Politics In The European Union*, European Journal on Criminal Policy and Research (Volume13, Issue 1-2), 2007, pp. 109-137, at p. 114.

[17] Robinson, Neil, Hans Graux, Maarten Botterman and Lorenzo Valeri, *Review Of The European Data Protection Directive*, Rand Europe, Brussels, 2009, at p. 16. Available online at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive_summary.pdf.

[18] Hornung, Gerrit, *The European Regulation On Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework And Technical Safeguards*, SCRIPT-ed (Volume 4, Issue 3), 2007, pp. 246-262, at p. 249. Available online at: http://www.law.ed.ac.uk/ahrc/script-ed/vol4-3/hornung.pdf.

and Development follows this line of reasoning, too. It states that "*security in Europe is a precondition of prosperity and freedom*."[19] Referring to information technology systems generally, the Commission also acknowledged that "[they] *can serve to protect and amplify the fundamental rights of the individual*".[20] In this way, European institutions ultimately defend the role they play in security as one of promoting human rights. These understandings are reminiscent of the theoretical approaches that do not consider rights and policies to be exclusive of one another, the former concerning the individual and the latter society, but see them as living in harmony.[21]

The conciliatory rhetoric also pervades the Commission proposals, presented on the 25 January 2012, aiming "*to build a modern, strong, consistent and comprehensive data protection framework for the European Union*".[22] In the Commission's own terms, this

[19] European Parliament and of the Council, Decision No 1982/2006/EC concerning the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007-2013), 18 December 2006. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:412:0001:0041:EN:PDF.

[20] European Commission, COM (2010) 609 final, at p. 2.

[21] Dworkin, Ronald, *Sovereign Virtue, The Theory and Practice of Equality*, Harvard University Press, Cambridge, 2002, at p. 23; Raz, Joseph, *Rights and Politics*, in: Tasioulas, John (ed.), *Law, Values And Social Practices*, Aldershot, Dartmouth, 1997, at p. 89.

[22] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final, 25 January 2012, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF; European Commission, Proposal for a Directive of

reform will first of all "*benefit individuals by strengthening their data protection rights*".[23] But, the Commission also purports to "*simplify the regulatory environment*" for businesses "*by drastically cutting red tape and doing away with formalities such as general notification requirements*".[24] Additionally, growing trust among law enforcement authorities is also sought "*to facilitate exchanges of data between them and cooperation in the fight against serious crime* […] *while ensuring a high level of protection for individuals*".[25]

Yet, beyond this pacifying discourse, what one really witnesses is, in our opinion, a determined move by the EU to foster the use of personal data for the sake of security with clear detrimental effects on the effectiveness of personal data protection principles and rights. As a matter of fact, the Commission has consistently shown its determination to improve the "*effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs*".[26] "*Security in the EU*", the Commission underscored, "*depends on effective mechanisms for exchanging information between national authorities and other European players*."[27] Apprehensive

the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012) 10 final, 25 January 2012, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF.

[23] European Commission, COM (2012) 11 final, at p. 8.

[24] European Commission, COM (2012) 11 final, at p. 12.

[25] European Commission, COM (2012) 11 final, at p. 8.

[26] European Commission, COM (2005) 597 final.

[27] European Commission, Communication to the European Parliament and the Council, *An area of freedom, security and justice serving the citizen*, COM (2009) 262 final, 10 June 2009, at p. 15.

with the “under-exploitation of existing systems”, the Commission has vigorously promoted extensive access by police and security services to information systems, for instance, by asylum and immigration authorities to VIS and SIS: “*In relation to the objective of combating terrorism and crime, the Council now identifies the absence of access by internal security authorities to VIS data as a shortcoming. The same could also be said for SIS II immigration and Eurodac data*.”[28]

A parallel trend can be noticed for continually broader categories of personal data to be included in these databases. From SIS I to SIS II (planned to start in 2013) digital prints and photographs, as well as biometrical data will be added to the system. Legal instruments facilitating the access to and exchange of information became a priority for the EU legislature.[29]

Concerns in respect of these developments have been voiced within the EU itself. Referring to the Commission proposal for a new legislation on requesting comparisons with Eurodac data by member states’ law enforcement authorities and EUROPOL,[30] the EDPS did

[28] European Commission, Proposal for a Council Decision on requesting comparisons with EURODAC data by member states' law enforcement authorities and Europol for law enforcement purposes, COM (2009) 344 final, 10 Setember 2009.

[29] Hijmans and Scirocco, *Shortcomings In EU Data Protection In The Third And The Second Pillars. Can The Lisbon Treaty Be Expected To Help?*, at p. 1487.

[30] European Data Protection Supervisor (EDPS), Opinion on the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of ‘Eurodac’ for the comparison of fingerprints for the effective application of Regulation (EC) (establishing the criteria and mechanisms for determining the member state responsible for examining an application for international protection lodged in one of the member states by a third-country national or a stateless person), and on the proposal for a Council Decision on

not conceal its uneasiness. Eurodac database was set up to identify asylum-seekers rather than to allow police to search for criminals. The Commission put forward this proposal following a request from member states, led by Germany, to allow their law enforcement authorities and Europol access to the Eurodac database to help investigations into terrorism and other serious crimes. For the EDPS, the proposal not only fits in the general trend to grant law enforcement authorities access to several large-scale information and identification systems. It also constitutes a further step in a tendency towards giving law enforcement authorities access to data of individuals who in principle are not suspected of committing any crime.[31] Moreover, it concerns data that have been collected for purposes that are not related to the combat of crime. Rather, the EDPS stressed, to be valid, the necessity of the intrusion must be supported by clear and undeniable elements, and the proportionality of the processing must be demonstrated:

> "*The systematic storage of the fingerprints of asylum seekers who have not been related to any crime in the same database with other fingerprints collected by law enforcement authorities — of asylum seekers and/or other persons suspected of crime or convicted — raises in itself serious concerns as to the purpose limitation principle and the legitimacy of data processing*."[32]

This is all the more required, the EDPS added, in case of an extensive intrusion in the rights of individuals

requesting comparisons with Eurodac data by member states' law enforcement authorities and Europol for law enforcement purposes (2010/C 92/01), 10 April 2010.

[31] EDPS, Opinion 2010/C 92/01, at p. 4.

[32] EDPS, Opinion 2010/C 92/01, at p. 5.

constituting a vulnerable group in need of protection, as foreseen in the proposal.

Remarkably, the EDPS points to the inconsistency between growing personal data gathering, use and transfer, and a political rhetoric where emphasis on human rights appears on the rise:

> "*The Commission explicitly deals with the compliance with fundamental rights, inter alia with Article 8 of the EU CFR. It explains that, … in order to ensure that the processing of personal data for law enforcement purposes does not contravene the fundamental right to the protection of personal data, in particular the necessity and the proportionality, the proposal sets out strict conditions.(…) The EDPS is not convinced by this statement of the Commission*."[33]

In the same vein, Rodotà alerted that Directive 2006/24/EC, rather than an exception to general rules, may turn out to be "*an anticipation of the future, the first stage for a deep change of the basic data protection principles*." The logic of reuse and interconnection or multifunctionality, prevails.[34] More than that, these developments occur with "*no real debate or analysis of the necessity or proportionality of measures taken for fighting terrorism and no real evaluation of the balancing vis-à-vis fundamental rights*".[35] It comes, therefore, as no surprise that scholars have baptized the society we live in as a "surveillance society", one that poses new threats for data

[33] EDPS, Opinion 2010/C 92/01, at p. 6.

[34] Rodotà, Stefano, *La Conservación De Los Datos De Tráfico En Las Comunicaciones Electrónicas*, Revista de Internet, Derecho y Política (Volume 3), 2006, pp. 53-60, at pp. 53-55.

[35] Rodotà, *La Conservación De Los Datos De Tráfico En Las Comunicaciones Electrónicas*, at p. 57.

protection and privacy.[36]

Against this backdrop, the question returns whether Article 8 of the EU Charter of Fundamental Rights, elevating the protection of personal data to the status of a fundamental human right, is resulting in a rebalancing of data protection principles and rights vis-à-vis the requirements of security.

D The Fundamental Right to Personal Data Protection: Does it Really Matter for Protecting Data in the Domain of Security?

As indicated, a latest breakthrough in this domain has been the granting of a constitutional standing to personal data protection by Article 8 of the EU Charter of Fundamental Rights, now an integral part of the EU law. Article 8 states that "*Everyone has the right to the protection of personal data concerning him or her*" and that "*Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law*".

The entry into force of the Lisbon Treaty marks a new era for data protection, the EDPS predicted. Article 16 of the Treaty on the Functioning of the EU not only contains an individual right of the data subject, but also provides a direct legal basis for a strong EU-wide data protection law. Furthermore, the abolition of the pillar structure obliges the European Parliament and the Council to provide for data protection in all areas of EU law, allowing for a comprehensive legal framework for data

[36] Hijmans and Scirocco, *Shortcomings In EU Data Protection In The Third And The Second Pillars. Can The Lisbon Treaty Be Expected To Help?*, at p. 1487.

protection applicable to the private sector, the public sector in the member states and the EU institutions and bodies.[37]

In the light of such optimistic expectations, one might expect that the European Treaties and the Charter could bring about a reshaping of EU data protection regimes. But is the upgrading of the right to data protection to a constitutional status having any perceivable effect on a rebalancing of the values and interests at stake?

In its recent proposals for a regulation and for a directive in this field[38] the Commission summons Article 8 of the Charter insistently, although signaling that the right to the protection of personal data is not an absolute right, but "*must be considered in relation to its function in society*".[39] Both proposals rely on the balancing discourse referred to above whereby protecting the fundamental rights and freedoms of natural persons and, in particular, their personal data, should not be regarded as incompatible with the growing use of these data either for economic or administrative purposes or for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.[40]

The proposed regulation, designed to replace the 1995 Data Protection Directive, is guided by concern for

[37] EDPS, Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, *A comprehensive approach on personal data protection in the European Union*, 14 January 2011, at p. 6. See also Blas, Diana Alonso, *First Pillar And Third Pillar: Need For A Common Approach On Data Protection?*, in: Gutwirth, Serge, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds.), *Reinventing Data Protection?*, Springer, The Netherlands, 2009.

[38] European Commission, COM (2005) 597 final.

[39] European Commission, COM (2012) 10 final, at p. 6.

[40] European Commission, COM (2012) 10 final, at p.2.

more harmonization of the data protection regime across member states and by the will to reinforce the mechanisms for institutional supervision and control.[41] This objective should be accomplished through the establishment of privacy officers in enterprises with more than 250 workers, the obligation to notify data breaches in no more than 24 hours, higher penalties for infringement, and the replacement of the Article 29 Data Protection Working Party, the independent EU Advisory Body on Data Protection and Privacy according to the Data Protection Directive, by a European Data Protection Board. The proposal also adds two novel rights to the existing ones, namely: a right to be forgotten and a right to data portability. The right to be forgotten has been approached as "*nothing more than a way to give (back) to individuals control over their personal data and make the consent regime more effective*"[42]. In these ways, a real reinforcement of data protection principles as well as of data subjects' rights may be achieved. Accordingly, De Hert and Papakonstantinou assent that "[t]*he replacement of the Regulation is an important and far-reaching development; once finalized, the new instrument is expected to affect the way Europeans work and live together*",[43] a "*definite cause for celebration for human rights*."[44]

The same authors, however, admit that the proposal endorses the move toward allowing the processing of personal information for purposes unforeseeable at the

[41] European Commission, COM (2012) 11 final.

[42] Ausloos, Jeff, *The 'Right To Be Forgotten' – Worth Remembering?,* Computer Law and Security Review (Volume 28), 2012, at p. 143.

[43] De Hert and Papakonstantinou, *The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System For The Protection Of Individuals*, at p. 131.

[44] Id., at p. 142.

time of data collection, to which evidently no consent has been given by the individuals concerned, thus undermining the principle of purpose specification. Furthermore, the “compatibility” criterion in the draft regulation is of little assistance, because in practice data controllers will be those deciding what is “compatible” or not, leaving it up to individuals the difficult task of taking action to challenge such decisions.[45]

Reservations are much stronger, however, with respect to the proposed Directive on the Protection of Individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

First of all, the choice of a separate instrument to regulate the processing of personal data in the police and judicial sectors has not been uncontroversial. The Commission indeed had two law-making options at hand while amending the EU Data Protection Framework: either to replace both the Directive and the Framework Decision with a single instrument or to amend each one of these. By choosing the second approach, the Commission gave rise to several criticisms. The EDPS argued that police and justice should be included in a single general EU legal instrument, preferably a regulation. A single instrument would give more guarantees to citizens, render the task of police authorities easier, as well as enabling data protection authorities the same extensive and harmonized powers vis-à-vis police and judicial authorities as they have regarding other data controllers.[46] “*In the area of data protection a Regulation is all the more justified, since*

[45] Id., at p. 135.

[46] EDPS, *A comprehensive approach on personal data protection in the European Union*, at pp. 11-26.

Article 16 TFEU has upgraded the right to the protection of personal data to the Treaty level and envisages – or even mandates – a uniform level of protection of individual throughout the EU."[47] A fundamental right to personal data protection should be meant as to protect citizens under all circumstances, the EDPS underlined. Moreover, the distinction between general and commercial data protection, on the one hand, and security-related personal data processing, on the other, is elusive. This is because datasets are increasingly created by private data controllers for their own purposes and may be accessed at some future point by law enforcement agencies. "*By insisting on two separate instruments for each type of processing, the Commission risks to prolong ambiguity in the field each time law enforcement agencies and the private sector interact*."[48]

With that option, the Commission eventually contradicted the comprehensive approach of its Communication, which paved the way for this reform. The Commission itself had stressed the need to ensure that the fundamental right to personal data protection is consistently applied in the context of all EU policies, including law enforcement and crime prevention as well as in international relations.[49]

[47] EDPS, *A comprehensive approach on personal data protection in the European Union*, at p. 9.

[48] De Hert and Papakonstantinou, *The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System For The Protection Of Individuals*, at p. 132.

[49] European Commission, Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, Delivering an area of freedom, security and justice for Europe's citizens Action Plan Implementing the Stockholm Programme, 20 April 2010, COM (2010) 171 final, p. 3. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:EN:PDF.

The projected Directive employs a rather permissive language in many of its provisions, directing member states to apply data protection principles in "*as far as possible*" or to provide that "*all reasonable steps*" are taken by controllers to comply with data subjects' rights (see, for instance, Articles 5, 6 and 10). While some of the recommendations advanced by the EDPS, for instance, for distinguishing between various categories of data subjects (criminal suspects, victims, witnesses etc.) have been incorporated in the draft directive, others have not been envisaged, including for specific conditions and safeguards to be foreseen for the processing of data of non-suspects or for specific safeguards to be devised in relation to the (increasingly relevant) processing of biometric in the field of law enforcement.

Of course, defending the data subject's fundamental right to data protection does not imply that data protection should always prevail over other important interests in a democratic society. Yet, it should have consequences for the nature and scope of the protection that must be given, so as to ensure that data protection requirements are always adequately taken into account, making it feasible for individuals to exercise their rights in practice, with limitations to the exercise of the right taken as exceptional, duly justified and never affecting the essential elements of the right.

In this light, the proposal for a directive also raises misgivings as to the balance reached. In contrast with the proposal for a regulation, the proposal for a directive contains a specific provision on the limitations of the right of access (Article 13, proposal for a regulation) admitting the adoption by member states of legislative measures restricting, wholly or partly, the data subject's rights. Besides, the principle of transparency in personal data processing, affirmed in the proposal for a regulation, has been excluded from the proposal for a directive (Article 5, a)).

According to the Charter, any restriction to fundamental freedoms and rights must be necessary and proportional in view of the goals pursued, namely fighting crime and terrorism (Article 52, Charter of Fundamental Rights). The EDPS admitted that limitations to the rights of data subjects may be foreseen, but they have to be necessary, proportionate and not alter the essential elements of the right itself. In addition, specific safeguards needed to be put in place, in order to compensate the data subject by giving him additional protection in an area where the processing of personal data may be more intrusive.[50]

The latest developments concerning the transfer of PNRs to other countries for security purposes have not gone without controversy, too.[51]Article 29 Data Protection Working Party and the EDPS considered these measures non-proportional since a great number of personal data are collected on all passengers regardless of the fact that they are under suspicion; and no statistical or other data were available to demonstrate their necessity.[52] The

[50] EDPS, *A comprehensive approach on personal data protection in the European Union*, at p. 17.

[51] Council of the European Union, Council Decision 2007/551/CFSP/JHA.

[52] Article 29 Data Protection Working Party, Opinion 10/2011 on the proposal of a directive of the European Parliament and the Council concerning the use of PNR for the purposes of prevention, detection, investigation and repression of terrorist and criminal acts, 2011. Available online at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp181_en.pdf; EDPS, Opinion on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, Brussels (2012/C 35/03), 9 December 2011. Available online at: http://eur-

simple argument of necessity and of general acceptance of PNR for combatting terrorism and serious crime, put forward by the Commission, was disallowed as insufficient to demonstrate the necessity of what was being proposed.[53] Other available means should have been explored preferably with less intrusive effects for *bona fide* passengers in order to ensure security in air travelling".[54]

To sum up, we may sceptically infer that the inclusion of the right to personal data protection in the EU Charter of Fundamental Rights has not been by itself sufficient to assure a data protection regime that resists criticism.

E Conclusion

Protection of personal data is one of the major legal issues facing present-day information society. Indeed, in the last decade, the reinforcement of security policies alongside the expansion of information systems and databases containing personal data designed for law enforcement and crime prevention caused mounting concerns from the human rights' standpoint. This concern was accentuated in the EU, by the apparent inadequacy of the existing legal basis in addition to the ostensive lack of proportionality as

lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:035:0016:0022:EN:PDF.

[53] European Commission, Proposal for a Directive of the European Parliament and the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM (2011) 32 final, 2011. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0032:FIN:EN:PDF.

[54] Article 29 Data Protection Working Party, Opinion 7/2010 on European Commission's Communication on the global approach to transfers of PNR data to third countries, 2010.

regards the quantity and the kind of data processed for security purposes, awakening fears about the emergence of a state-controlled surveillance society. Amazingly, the EU institutional discourse has regularly presented security and human rights as if they were the two sides of the same coin. However, this conciliatory approach appears to be contradicted by the ways in which EU security policies have been impacting upon the protection of personal data regimes, giving rise to rather ambiguous feelings.

The recent adoption of the EU Charter of Fundamental Rights, including a fundamental right to the protection of personal data, opened up reasonable expectations for a rebalancing of the requirements of EU security policies vis-à-vis personal data protection principles and rights, and paved the way for the ongoing reform of EU data protection regimes. However, whereas the 2012 Commission's proposal for a new regulation, submitted under the Internal Market provisions of the EU Treaty, is being regarded by some observers as a "*cause for celebration for human rights*"[55], the proposal for a new directive under the EU Area of Freedom, Security and Justice has been received unenthusiastically. Reservations have been voiced, first of all, concerning the two legal instruments option, a regulation and a directive, thought to hamper an uniform, consistent level of protection of individuals throughout the EU, allowing data protection authorities the same extensive and harmonized powers as regards police and judicial authorities as they have for other data controllers. The degree of flexibility permitted by the language of the proposal for a new directive also caused apprehension.

Eventually, expectations opened up by the adoption of Article 8 of the Charter of Fundamental Rights end up unfulfilled to a considerable extent.

[55] See note 44 above.

The purpose limitation principle and data minimization policies, both in the public and the private sector, and the rights of the data subject need to be more effectively safeguarded if a sounder equilibrium between the important values at issue, and an effective promotion of the fundamental rights are to be achieved in a more and more complex societal and technological environment.

IV Recent Developments

Matthias C. Kettemann[*]

The UN Human Rights Council Resolution on Human Rights on the Internet: Boost or Bust for Online Human Rights Protection?[**]

Abstract

Human rights play a central role on the Internet. They are the base layer on which human security in the information society can be ensured and the normative foil against which human security assessments of national (and international) Internet Governance policies can be conducted. In July 2012, the UN Human Rights Council has passed a key resolution confirming that the same human rights that people enjoy offline must also be protected online. The contribution parses the resolution and engages in a critical review of its main points. While the commitment to human rights protection will be identified as an important boost for human rights, the Council failed to more clearly lay down the limits to state limitations of human rights online. The contribution will conclude with the call to take the resolution as a starting point to operationalize the commitment to

[*] Dr. Matthias C. Kettemann, LL.M. (Harvard), is research and teaching fellow at the Institute of International Law and International Relations of the University of Graz, Austria, and co-chair of the Internet Rights and Principles Coalition. He blogs about international legal challenges of the information society at http://internationallawandtheinternet.blogspot.com; E-mail: matthias.kettemann@uni-graz.at.

[**] An abbreviated version of this contribution was published as Kettemann, *UN Human Rights Council Confirms that Human Rights Apply to the Internet*, in EJIL Talk, 23 July 2012, http://www.ejiltalk.org/un-human-rights-council-confirms-that-human-rights-apply-to-the-internet/#more-5207.

human rights online, a process that can be helped by the interpretative impact of human security. The concept, in turn, will be influenced by the evolution of Internet rights and principles.

Keywords: Human Security, Human Rights online, Internet Governance, Access, Openness, Internet Architecture, International Internet Law

A Introduction

Both human security and human rights have been deeply impacted by the emergence of information and communication technologies, the rise of the networked society, and the needs for self-actualization of the digital natives.[1] In his contribution, Wolfgang Benedek has explained what challenges human security is confronted with in the process of governing the Internet.[2] Human security and human rights share intricate interlinkages, but are two distinct concepts.[3] “Whereas human security requires a political commitment”, as Benedek writes, “human rights must be respected by states and often also non-state actors as binding law.”[4] In order to ensure

[1] See already Benedek, Wolfgang and Catrin Pekari (eds*.), Menschenrechte in der Informationsgesellschaft* [Human Rights in the Information Society], Boorberg, Stuttgart, 2006; and Jørgensen, Rikke Frank (ed.), *Human Rights in the Global Information Society*, MIT Press, Cambridge, MA, 2006.

[2] Cf. Benedek, Wolfgang, *Human Security in the Information Society*, in this journal, supra.

[3] Cf. Kettemann, *Harmonizing International Constitutional Law and Security: the Contribution of the Concept of Human Security*, in Eberhard, Harald, Konrad Lachmayer, Gregor Ribarov and Gerhard Thallinger (eds.), *Constitutional Limits to Security. Proceedings of the 4th Vienna Workshop on International Constitutional Law*, Nomos, Vienna/Baden-Baden, 2009, at pp. 109-134.

[4] Benedek, in this journal, supra.

human security in the information society, we need to have a firm base layer of human rights which allow us to develop more human security-sensitive national Internet policies.

I shall therefore focus in this contribution on the role of human rights in the Internet and will, more specifically, assess the impact of the UN Human Rights Council Resolution confirming the extension of offline rights to online settings.

On 5 July 2012, the UN Human Rights Council (HRC) adopted by consensus a key resolution on promotion, protection and enjoyment of human rights on the Internet.[5] Presented by Sweden the Resolution enjoyed broad international backing from more than 70 HRC member countries and non-members from all regional groups, including China, Brazil, Nigeria, Ukraine, Tunisia, Turkey, the United States and the United Kingdom.

Centrally, the Resolution affirms in its operative para. 1 that "the same rights that people have offline must also be protected online" and should thus put to rest the tedious debate about whether we need 'new' human rights for the Internet age, motivated chiefly by states not wishing to ensure the 'old' human rights in an online environment.[6]

[5] UN Human Rights Council, Resolution: The promotion, protection and enjoyment of human rights on the Internet, A/HRC/20/L.13, 29 June 2012 [draft] (adopted on 5 July 2012).

[6] Cf. Matthias C. Kettemann, *The Power of Principles: Reassessing the Internet Governance Principle Hype*, in: Schweighofer, Erich, Franz Kummer and Walter Hötzendorfer (eds.), *Transformation jurstischer Sprachen* [Transformation of Legal Languages]. *Tagungsband des 15. Internationalen Rechtsinformatik Symposions IRIS 2012* [Proceedings of the 15th International Legal Informatics Symposion], Vienna 2011, at pp. 445-448.

The importance of ensuring human rights protection on the Internet cannot be overestimated. The Internet has become “a catalyst” for individuals all across the world to exercise a broad range of human rights, both directly, such as the rights to freedom of expression and assembly, and indirectly, in that the Internet facilitates the realization of human rights ranging from health to education, from food to development.[7]

Though the Resolution’s approach is sound, I will take issue with a number of points, identify remaining problems and discuss priorities for the international political process, including chiefly the need to prioritize international discussions on how international law protects human rights online and what obligations are incumbent upon states when it comes to ensuring the Internet’s stability, security and functionality. In conclusion, I will offer some perspectives on the future evolution of the human rights protection framework in the Internet age.

B The HRC Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet

The Resolution contains five preambular and five operative paragraphs. In the five preambular paragraphs the HRC refers to the guiding power of the Charter of the United Nations (PP1) and reaffirms the human rights and fundamental freedoms enshrined in the Universal Declaration of Human Rights and international human

[7] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27, 2011, at para. 22.

rights treaties, including the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights (PP2).

The HRC further refers to previous resolutions by different UN bodies on freedom of opinion and expression (PP3) and, notably, a recent UN General Assembly resolution on Information and communications technologies (ICTs) for development.[8]

The Council subsequently notes that in light of the quick pace of technological development questions regarding the exercise of human rights, in particular the right to freedom of expression, on the Internet grow in importance (PP4). Finally, it takes note of two milestone reports from 2011 of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (to the Human Rights Council[9] and to the General Assembly[10]) that contain a roadmap for states to human rights-sensitive Internet policy-making.

The five operative paragraphs are brief enough to merit full citation. They run as follows:

> “*The Human Rights Council* […]
>
> *1. Affirms that the same rights that people have offline must also be protected online, in particular*

[8] UN General Assembly, Resolution 66/184 on Information and communications technologies for Development, A/RES/66/184, 6 February 2012.

[9] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.

[10] UN General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/66/290, 2011.

> *freedom of expression, which is applicable regardless of frontiers and through any media of one’s choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights;*
>
> *2. Recognizes the global and open nature of the Internet as a driving force in accelerating progress towards development in its various forms;*
>
> *3. Calls upon all States to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries;*
>
> *4. Encourages special procedures to take these issues into account within their existing mandates, as applicable;*
>
> *5. Decides to continue its consideration of the promotion, protection and enjoyment of human rights, including the right to freedom of expression, on the Internet and in other technologies, as well as of how the Internet can be an important tool for development and for exercising human rights, in accordance with its programme of work.*”

I will address each in turn, contextualize its content in light of both the human rights and the Internet Governance debates, and, where necessary, identify open questions and shortcomings.

C The Commitment to Human Rights Online (para. 1)

In its first operative paragraph the Human Rights Council affirms “that the same rights that people have offline must also be protected online”. This is what the Resolution boils down to. Offline human rights apply online and states have a duty to protect them. More generally, they have a duty to respect, protect and implement them, as they do with regard to all other human rights.

This basic tenet for the information society is sound. Human rights are the loadstar for Internet policy-making. There is no need to reinvent human rights. Rather, they have to be applied to Internet-related cases in light of online challenges.

The Resolution names one human right that has a particularly important role on the Internet: freedom of expression. Indeed, the Internet has become, in Special Rapporteur Frank La Rue’s turn in his seminal 2011 report to the Council, a “key means” through which freedom of expression can be exercised.[11] The right to freedom of expression is not only a human right by and of itself but also enables the enjoyment of other human rights, namely (per Frank La Rue)

> “*economic, social and cultural rights, such as the right to education and the right to take part in cultural life and to enjoy the benefits of scientific progress and its applications, as well as civil and*

[11] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, at para. 20.

> *political rights, such as the rights to freedom of association and assembly.*"[12]

The Council specifically refers to freedom of expression and cites the language of Article 19 of the Universal Declaration of Human Rights (UDHR) which guarantees everyone

> "*the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.*"

The Article's language is based on technological neutrality – vide "through any media" – and the recognition of the importance of entering into universal processes of seeking and imparting information and ideas – vide "regardless of frontiers". It thus seems to have anticipated developments in ICTs and the growing internationalization of content flows.

The Resolution also references Article 19 of the International Covenant on Civil and Political Rights (ICCPR) which is more detailed in its wording and contains restriction which are prone to be misused by states seeking to exercise control over online expression. Article 19, para. 1, ICCPR guarantees the right to hold opinions without interference. Para. 2 enshrines the right to freedom of expression, including the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in

[12] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, at para. 22.

the form of art, or through any other media of [one's] choice." Note, again, the dual preconditions of technological neutrality – "through any [media] of [one's] choice" – and the universality of the information processes – "regardless of frontiers".[13]

Unlike the UDHR, Article 19, para. 3, ICCPR allows for certain restrictions of the right which have to be "provided by law and […] necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals."

In 1996, Internet activist John P. Barlow published his Declaration of the Independence of Cyberspace, where he claimed that states had "no moral right to rule us [the citizens of cyberspace] nor do you [the states] possess any methods of enforcement we have true reason to fear."[14] The moral right to rule and restrict Internet-related human activity always existed for states, but only within the bounds of international law, and by 2012 states do possess enforcement methods that seriously endanger the enjoyment of human rights on the Internet.

No one doubts that illegal content has to be effectively fought and that it has to be primarily states, in cooperation with other stakeholders, and sensibly self-regulated Internet Service Providers, search engine

[13] Cf., on the many dimensions of the protection of communication acts in the information society, Schmalenbach, *Ein Menschenrecht auf Kommunikation: Erfordernis oder Redundanz?* [A Human Right to Communication: Necessary or Redudant?], in Benedek and Pekari (eds.), *Menschenrechte in der Informationsgesellschaft*, at p.183.

[14] Barlow, John Perry, *A Declaration of the Independence of Cyberspace*, Davos, 8 February 1996. Available online at: http://www.actlab.utexas.edu/~captain/cyber.decl.indep.html (All websites used in this essay were last checked on 1 August 2012).

providers and social networking providers who have to lead the fight. The fight, however, must not be used by states as a fig leaf for widespread censorship. This is a lamentable lacuna in the resolution and states were quick to pick up on it in the process leading up to it adoption.

In the debate in the Council, China stressed that

> "*online gambling, pornography and hacking were increasingly becoming a threat to the legal rights of society, particularly minors. States therefore were bound to run the Internet legally, otherwise the free flow of unhealthy and negative information would obstruct the function of the Internet.*"[15]

The 'function' of the Internet cannot be to be a clean, completely safe, and conflict-free zone of unlimited consumerism. Further, the exact meaning of "unhealthy and negative information" is open to debate. Authoritarian countries would probably find democracy-promotion unhealthy and open critique of their human rights records negative.

Rather, states are obliged to respect the rights enshrined in the Covenant and the UDHR and foresee, in their national legislation, only for those limitations which are legitimate under human rights law.

Both UDHR and ICCPR can thus be interpreted to allow restrictions only be provided by a *clear law* that is accessible to all, must be aim to ensure of the *legitimate purposes* (as contained in Article 19, para. 3) and be

[15] Office of the High Commissioner for Human Rights, *Council appoints a Special Rapporteur on Belarus, adopts 12 resolutions on promotion and protection of all human rights*, 5 July 2012. Available online at: http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=12323&LangID=E.

necessary for that protection and proven to be the *least restrictive* means required to achieve the purported aim. In its 2011 General Comment No. 34 on Article 19, the Human Rights Committee overseeing the Covenant underscored that states "must demonstrate in specific fashion the precise nature of the threat to any of the enumerated grounds listed in paragraph that has caused it to restrict freedom of expression".[16]

Pursuant to the General Comment the specificity of the threat against a legitimately protected public good, as enumerated in Article 19, para. 3, also applies to all actors and forms of interaction relevant on the Internet: specifically, "websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines […]". Further, generic bans are never compatible with the exception regime of para. 3, nor is the prohibition of criticism of the government or of the state's political system.[17]

This leads us to an important trifurcation: As the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression wrote in his report to the General Assembly in 2011, three types of expressions (and state reaction to it) need to be kept strictly apart:

> "*(a) expression that constitutes an offence under international law and can be prosecuted criminally;*

[16] UN Human Rights Committee, General Comment No. 34, Article 19: Freedoms of opinion and expression, CCPR/C/GC/34, 2011, at para. 36.

[17] UN Human Rights Committee, General Comment No. 34, Article 19: Freedoms of opinion and expression, at para. 43.

> *(b) expression that is not criminally punishable but may justify a restriction and a civil suit; and*
> *(c) expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility and respect for others*."[18]

States are obliged to prohibit content falling under category (a). The category includes expression that is prohibited by international law:

- images of sexual exploitation of children (to protect the rights of children);
- advocacy of national, racial or religious hatred amounting to incitement to discrimination, hostility or violence (to protect the rights of others, such as the right to life);
- direct and public incitement to commit genocide (to protect the rights of affected communities); and
- incitement to terrorism.[19]

In his report, the Special Rapporteur also included defamation in this category,[20] but later argued, convincingly, that it should rather not be criminalized

[18] UN General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, at para. 18.

[19] UN General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, at paras. 20-36.

[20] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, at para. 25.

because of the potential chilling effect on freedom of expression.[21]

Of course, states also have to ensure that they provide for a system of laws and courts that allows those victimized by expressions under (b) to file for civil liability. With regard to civility-offences under (c), states have an important role of awareness-raising and should, rather than criminalize such expressions, address the underlying causes of discrimination in their society.[22]

Illegal content should thus be dealt with by authorities in line with their international obligations. Other content may be harmful, offensive, objectionable, or undesirable – but should not be target of state censorship. It is precisely these ideas that need protection. Ideas that in the words of the European Court of Human Rights in Handyside v. UK, words that reverberate across the ages and technologies, “shock, offend and disturb” a society or parts of it.[23]

Moreover, the affirmation that “the same rights that people have offline must also be protected online” in para. 1 of the HRC Resolution also extends to rights other than freedom of expression. But what are these rights?

In preambular para. 1 the Council sheds some light on the rights to be applied online by referring to the totality of

[21] UN General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, para. 40.

[22] UN General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, para. 40.

[23] Cf. European Court of Human Rights, *Handyside v. the United Kingdom* (no. 5493/72), 7 December 1976, para. 49.

> "*human rights and fundamental freedoms enshrined in the Universal Declaration of Human Rights and relevant international human rights treaties, including the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights* [...]*.*"

Of course, all other international human rights treaties are applicable as well, if states have ratified them or if they have crystallized into international customary law.

D A Global and Open Internet as a Facilitator of Development (para. 2)

In para. 2, the Human Rights Council recognizes both the "global and open nature of the Internet" as an important force in ensuring development. That the Internet, and ICTs more generally, are drivers of development has already been previously confirmed by the General Assembly. In its resolution on ICTs for development,[24] however, the General Assembly manages to not include a single reference to "human rights" in over seven pages. On UN level, the Human Rights Council thus establishes an important link. But the globality and openness of the Internet is not only a means to an end (development), but also has intrinsic value.

The casual recognition of the "global and open nature of the Internet" is important, as well, because of the current lack of legal protection that the Internet's openness enjoys in international law. Though references abound in

[24] UN General Assembly, Resolution 66/184 on Information and communications technologies for Development.

Internet-related documents, it is probably the Council of Europe (internationally renowned by now for innovative human rights responses to ICT-based challenges[25]) with its Declaration by the Committee of Ministers on Internet Governance principles of 21 September 2011 (CoE IGPs) that most authoritatively (and convincingly) delineates the connection between globality, openness, and other architectural principles of the Internet and human rights.[26]

The "global […] nature of the Internet" is premised upon both its universality and universal access (more on the latter in the next section). Experience counsels that any global common good needs to be protected by global policies. The Internet as a global common good demands global international law-based Internet (Governance) policies. These must ensure the unimpeded flow of transboundary Internet traffic (principle 5 of the CoE IGPs). While global policies for Internet *Governance* are

[25] Cf. Kettemann, *Ensuring Human Rights Online: An Appraisal of Selected Council of Europe Initiatives in the Information Society Sector in 2010*, in Benedek, Wolfgang, Florence Benoît-Rohmer, Wolfram Karl and Manfred Nowak (eds.), *European Yearbook on Human Rights 2011*, NWV, Vienna, 2011, at pp. 461-482; and Kettemann, Matthias, *Internet Governance and Human Rights in Europe*, in: Benedek, Wolfgang, Florence Benoît-Rohmer, Wolfram Karl and Manfred Nowak (eds.), *European Yearbook On Human Rights 2010*, NWV, Vienna, 2010, at pp. 335-352. For a broader overview of Council of Europe activities in the information society field, see Benedek, Wolfgang and Matthias C. Kettemann, *The Council of Europe and the Information Society*, in: Kicker, Renate (ed.), *The Council of Europe: Pioneer and Guarantor for Human Rights and Democracy*, Council of Europe, Strasbourg, 2010, at pp. 88-93.

[26] Committee of Ministers of the Council of Europe, Declaration by the Committee of Ministers on Internet Governance principles, 21 September 2011. Available online at: https://wcd.coe.int/ViewDoc.jsp?id=1835773.

necessary, the day-to-day *management* can and should remain decentralized (principle 7).[27]

A commitment to an ‘open’ Internet includes a commitment to open *standards* and to an open *network* (principles 8 and 9 of the CoE IGPs). Open standards and interoperability of the Internet, including its end-to-end-nature, are key architecture principles of the Internet which underlay the Human Rights Council’s commitment to its openness. The commitment to an open Internet in the sense of an open network is more clearly linked to human rights. This is well illustrated by principle 8 of the CoE IGPs, according to which user should have

> “*the greatest possible access to Internet-based content, applications and services of their choice, whether or not they are offered free of charge, using suitable devices of their choice.*”[28]

The link to human rights is clear: “Traffic management measures which have an impact on the enjoyment of fundamental rights and freedoms […] must meet the requirements of international law […].”[29]

E Facilitating Access and International Cooperation to Develop ICTs (para. 3)

In the Resolution’s third operative paragraph the Human Rights Council calls upon states to promote and facilitate *access* to the Internet and *international cooperation* with

[27] Cf. Ibid.

[28] Cf. Ibid.

[29] Cf. Ibid.

the goal to develop both media and information and communications facilities globally.

Ensuring access is indeed one of the key elements of human rights protection online. Neither access nor international cooperation are only means to the end of developing media and information and communications facilities.[30] They are both also values in themselves in light of their importance for evolution of the Internet.

There are two dimensions of access which have to be simultaneously pursued: physical access to the Internet, i.e. an Internet connection, and access to online content, that is access to unfiltered information online. The latter is protected by human rights law, especially the right to freedom of expression that limits state censorship (as elaborated with regard to para. 2, supra). The former is premised upon bridging the digital divide, the gap between those who have access and those who have not, but is intrinsically linked to all other human rights as a precondition for their exercise.

Increasing physical access and ensuring a higher level of Internet connection worldwide is therefore not only an obligation of each individual state but also of the international community as a whole. Or, as Tunisia put it in the Council debate, "the Internet as a vector for the enjoyment of human rights with enormous potential and [...] access to it should be guaranteed for everyone."[31] Indeed, bridging the digital divides is essential for ensuring

[30] 'Technologies, as in Information and Communication Technologies would have corresponded to the more common usage, while the reference to 'facilities' points to a more infrastructure-oriented approach.

[31] Office of the High Commissioner for Human Rights, *Council appoints a Special Rapporteur on Belarus, adopts 12 resolutions on promotion and protection of all human rights*.

that the Internet can have the catalytic impact on the enjoyment of all human rights.

As Internet access is closely linked to development, notably in the HRC's Resolution, Article 2, para. 1, of the International Covenant on Economic, Social and Cultural Rights (ICESCR) can be used as the normative frame in which national and international policies targeted at increasing physical Internet access are designed. Pursuant to that paragraph, states need to

> "*take steps, individually and through international assistance and co-operation, especially economic and technical, to the maximum of its available resources, with a view to achieving progressively the full realization of the rights recognized in the present Covenant by all appropriate means, including particularly the adoption of legislative measures.*"

These "appropriate means" include also close cooperation with the private sector in the implementation of transnational corporations responsibility for human rights in light of the Ruggie report.[32] At the same time, Article 2, para. 2, of the ICESCR ensures that extending Internet access be process without "discrimination of any kind as

[32] Cf. Ruggie, John, Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, UN Doc. UN A/HRC/17/31 of 21 March 2011. Cf. also Taylor, Mark B., *The Ruggie Framework: Polycentric regulation and the implications for corporate social responsibility*, Etikk i praksis. Nordic Journal of Applied Ethics (Volume 5, Issue 1), 2011, pp. 9-30.

to race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status." This is particularly important since there exist, in fact, not only a digital divide between developed and developing states, but rather multiple digital divides also within society, between the rich and poor, the traditionally and differently abled, the young and the elderly, and a gender gap.

International cooperation is not only essential in order to ensure access, but is also key to the security, stability, robustness and resilience of the Internet. National and international multi-stakeholder co-operation is essential for ensuring that Internet Governance policies are legitimate and human rights-sensitive. Unfortunately, the Resolution is silent on the importance of cooperation, and the role that multistakeholderism must play in international Internet Governance processes.[33]

This is problematic because a number of states conceive of cooperation in Internet Governance as a *multilateral*, i.e. state-based (as opposed to *multistakeholder*-based) affair. In a statement during the Council Debate, Brazil, for instance, welcomed the Resolution, but underlined that "[d]emocratic governance for the Internet was essential for the full enjoyment of this technological

[33] And not only there, see Benedek, Wolfgang, *The Relevance of Multi-Stakeholder Approach and Multi-Track Diplomacy for Human Rights Diplomacy*, in: O'Flaherty, Michael, Zdzislaw Kedzia, Amrei Müller and George Ulrich (eds.), *Human Rights Diplomacy: Contemporary Perspectives*, Nijhoff, Leiden/Boston, 2011, pp. 251-261, at. p. 253; and, regarding international law more generally, Benedek, Wolfgang, *Multi-Stakeholderism in the Development of International Law*, in: Fastenrath, Ulrich, Rudolf Geiger, Daniel-Erasmus Khan, Andreas Paulus, Sabine von Schorlemer and Christoph Vedder (eds.), *From Bilateralism to Community Interest. Essays in Honour of Bruno Simma*, OUP, Oxford, 2011, at pp. 201-210.

tool."[34] This is a Trojan horse insofar as references to "democracy" and "democratic" decision-making in Internet Governance usually mean that states should play a bigger role, as they are considered (notably by states, incidentally) as the only vessels through which democratic legitimacy can be challenged. But rather than multi*lateral*, a human rights-sensitive Internet Governance is multi*stakeholder*-based.

F Housekeeping (paras. 4 and 5)

In paras. 4 and 5, the Human Rights Council engages in intellectual housekeeping. First, it encourages its special procedures[35] to take the commitment to ensuring human rights online "into account within their existing mandates, as applicable" (para. 4).

Indeed, the Resolution's commitment to ensuring human rights online is applicable, albeit to varying degrees, to almost all of the 36 thematic and 12 country mandates of the HRC:[36] be it the Special Rapporteur on the right to education (Internet access as a precondition of using online learning resources), the Special Rapporteur on the rights to freedom of peaceful assembly and of association (including in its ambit social activism on the Internet) or the the Special Rapporteur on the situation of

[34] Office of the High Commissioner for Human Rights, *Council appoints a Special Rapporteur on Belarus, adopts 12 resolutions on promotion and protection of all human rights*.

[35] Office of the High Commissioner for Human Rights, Special Procedures, Available online at: http://www.ohchr.org/EN/HRBodies/SP/Pages/Welcomepage.aspx.

[36] Office of the High Commissioner for Human Rights, Special Procedures.

human rights defenders (who use the Internet intensively to publicize human rights violations).

But also country mandate-holders will need to focus (more) on the role of Internet censorship as a tool of oppression in 'their' countries. This applies especially to the newly appointed Special Rapporteur on the situation of human rights in Belarus and the Special Rapporteurs for Iran (where intensive filtering takes place), Myanmar (where the government has engaged in partial Internet shutdowns in the past) and Syria (where the Internet is used as a tool against the opposition).[37]

Though the right to freedom of expression is admittedly of overarching importance in the Internet, all mandate holders should nevertheless strive to emulate the technology-sensitive and holistic approach used by that right's Special Rapporteur, Frank La Rue, in his two key reports on the extent of, and the limits to, freedom of expression on the Internet.

In the Resolution's final paragraph (para.5), the Human Rights Council confirms that it will remain seized of the matter, and focus on both the overall issue of promotion, protection and enabling the enjoyment of human rights, including the right to freedom of expression, on the Internet, but also of the impact of the Internet on development and for exercising human rights.

[37] Cf., for an introduction into filtering and international law, Rundle, Mary and Malcolm Birding, *Filtering and the International System: A Question of Commitment*, in: Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain (eds.), *Access Denied. The Practice and Policy of Global Internet Filtering*, Harvard University Press, Cambridge (MA), 2008, pp. 73-101, at p. 74.

G Conclusion and Perspectives

The commitment to ensuring all human rights for all in a technology-neutral way, online just as offline, was an important first step by the Human Rights Council. States need to respect human rights online (and offline) and are only allowed to make recourse to the traditional exceptions provided by international human rights law. These exceptions must be narrowly tailored, specific and meet the traditional three-part-test: they need to be (1) provided by law (principle of legality), (2) targeted at achieving a legitimate goal (principle of legitimacy), and (3) necessary for achieving that goal and proportionate (principle of proportionality [and least intensive means]).

What needs to follow now is thus not an exercise in finding new rights, but rather in establishing how existing human rights are becoming relevant for the whole gamut of human activity online. In this process, the concept of human security can function as an important guiding principle for interpretation. These must be based on a parsing of existing human rights norms, developed in light of the technological challenges of information society and the socio-political changes that ICTs have brought along.

Civil society organizations, such as the Civil Society Internet Governance Caucus, have started to highlight the special challenges of applying pre-Internet rights to an Internet age and have collected lists[38] of statements and declarations on human rights on the Internet.

One of the most holistic is the Charter on Internet Rights and Principles[39] of the Internet Rights and

[38] Civil Society Internet Governance Caucus, List of Rights and Principles for the Internet. Available online at: http://igcaucus.org/links.

[39] Internet Rights and Principles Coalition, Charter on Internet Rights and Principles (2011), http://irpcharter.org.

Principles Coalition which also exists in an abbreviated version: the 10 Rights and Principles for the Internet. These rights can be useful as signposts on the way to the operationalization of human rights on the Internet.

One example is the right to access in its dual dimensions which truly undergirds all human self-actualization online and the realization of all other human rights. The Resolution underlines the importance of access and Article 1 of the Charter shows which human rights dimensions access can be understood to encompass:

- ever increasing quality of service in in line with advancing technological possibilities;
- freedom of choice of system and software use (including interoperability of protocols);
- ensuring digital inclusion; and
- Internet neutrality and equality.

Implementing these interconnected and mutually reinforcing aspects of the right to access presupposes taking different normative steps, both nationally and internationally and ensuring an ICT-sensitive judiciary. Indeed, every one of these aspects of access is covered by the right to access, as properly understood and applied to the Internet.

During the HRC debate, China referred to the “function” of the Internet. Though I doubt that we can agree on a specific function, and the argument that the Internet is a network of networks and thus function-neutral is rather compelling, the notion is interesting insofar as it allows us to look at the Internet in a functional way. If we do that, we should consider it as a tool to ensuring a higher level of human rights protection – online, for sure, but offline as well, as the events of the Arab Spring and the increasing use of the Internet by human rights defenders and for social activism have amply illustrated.

In an op-ed comment in the New York Times, Carl Bildt concludes

> "*The governments of the Human Rights Council now for the first time have confirmed that freedom of expression applies fully to the Internet.* […] *The challenge now is to put these words into action to make sure that people all over the world can use and utilize the power of connectivity without having to fear for their safety. This work is far from over.*"[40]

I agree. We need to put these words into actions. But, I would argue, we also need to put some more flesh on these words. What exactly does it mean for states that human rights that apply offline also apply online? That they have to respect, protect and implement them, and – as a precondition – increase Internet access in both dimensions: access to infrastructure and content.

What follows? Going on step further, we need to ensure that offline international law also applies online. What the Human Rights Council failed to do (but where we can take some inspiration from the Council of Europe's list of Internet Governance principles) is to clarify what human rights-based duties of states exist vis-à-vis the Internet: arguably to ensure its stability, functionality and integrity and, for that purpose, engage in cooperation with other states and develop national Internet policies that infringe

[40] Bildt, Carl, *A Victory for the Internet*, in *New York Times*, 5 July 2012. Available online at: http://www.nytimes.com/2012/07/06/opinion/carl-bildt-a-victory-for-the-internet.html?_r=1.

neither upon the human rights of its citizens nor violate emerging international legal obligations.[41]

This is not the end of the debate, neither is it the beginning. Rather, it is the end of the beginning (where the extent of human rights online was doubted by some states). Thanks to the Human Rights Council, we now have a clear yardstick against which future national and international policy-making bearing on Internet and human rights can be measured.

With the stage now set for the operationalization of the commitment to human rights online, the concept of human security in the information society, as discussed in the contributions in this volume will be immensely important to inform the interpretation of human rights online and to limit states' limits on online freedoms.

Concluding, the Human Rights Council Resolution was a boost for human rights as it pushes their protection further into the limelight of international discourse. It is in this process that the concept of human security in the information society plays an important informative role and will, in turn, be influenced by the evolution of Internet rights and principles. Thus, a human rights-based International Internet Law can solidify.

[41] Cf. Kettemann, Matthias C., *Gibt es Schutzlücken im Internet?* [Are there Human Rights Gaps on the Internet?], in: Gahren, Isabel, Sebastian Haselbeck, Matthias C. Kettemann and Max Senges (eds.), *Human Rights and the Internet. Access, Freedom, Control. Final Report of the 5th Initiative of the Internet& Society Co:llaboratory*, Internet&Society Co:lla-boratory, Berlin, 2012, at pp. 26-34. Available online at: http://cobase.collabora tory.de/w/Abschlussbericht_Menschen rechte_und_Internet.

University of Graz
Institute of International Law
and International Relations

National Defence
Academy
Republic of Austria

UNIVERSITY OF GRAZ
EUROPEAN TRAINING & RESEARCH CENTER
FOR HUMAN RIGHTS AND DEMOCRACY

Österreichisches Institut
für Internationale Politik
Austrian Institute for
International Affairs

University of Graz
HUMAN SECURITY
FOCUS GROUP

SPBUILD:
Sustainable Peace Building

MARIE CURIE ACTIONS

SEVENTH FRAMEWORK
PROGRAMME

5th Graz Workshop on the Future of Security

Human Security in the Information Society: Regulating Risks – Empowering People

© CC hdzimmermann (Flickr)

Friday, 16 March 2012
University of Graz, Austria

5th Graz Workshop on the Future of Security

Human Security in the Information Society: Regulating Risks – Empowering People

Friday, 16 March 2012 | University of Graz, Austria

RESOWI Center A2, SZ 15.21

Programme

8:00 **Registration**

9:00-9:15 **Welcome remarks**
Joseph Marko
Dean, Faculty of Law, University of Graz, Austria

9:15-10:15 **Keynote Session I: Human Rights, Technology and Online 'Securities'**

Human Security in the Information Society
Wolfgang Benedek
Institute of International Law and International Relations and European Training and Research Center of the University of Graz, Austria

The Threats of Social Engineering and Malicious Insiders to IT Security
Wolfgang Slany
Institute for Software Technology, Technical University Graz, Austria

10:15-10:45 **Coffee break**

10:45-12:15 **Thematic Session I: Ensuring Human Security Online: the Rights Approach**

Chair: **Wolfgang Benedek** (Graz, Austria)

Are Internet Governance Principles the New Pathway to Human Security and Human Rights Online?
Matthias C. Kettemann (Graz, Austria)

Security and the Right to Data Protection in the EU
Maria Eduarda Gonçalves / Inês Andrade Jesus (Lisbon, Portugal)

Balancing Rights in the Information Society: Human Rights and the Protection of Public Security
Cristina Pace (Graz, Austria / Lisbon, Portugal)

12:15-13:30 **Lunch break**

13:30-14:30 **Keynote Session II: Political Contributions and Military Challenges to Human Security in the Internet Age**

Military Security, Human Security and the Internet
Ernst M. Felberbauer
Head of Research Management, National Defence Academy, Ministry of Defence and Sports, Austria

How the European Parliament Safeguards Human Rights on the Internet
Jörg Leichtfried
Member of the European Parliament, President of the Delegation of the Social Democratic Party of Austria to the European Parliament

14:30-15:00 **Coffee break**

15:00-16:30 **Thematic Session II: Ensuring Human Security Online: Technological Challenges and Regional Dimensions**

Chair: **Wolfgang Slany** (Graz, Austria)

Functional Magnetic Resonance Imaging and the Challenge of Balancing State Security with Human Security
Farhan Sahito (Graz, Austria)

Securitization in Internet Governance: Testing the Copenhagen School's Approach
Philipp Mirtl (OIIP, Austria)

Challenges to Empowering Civil Society and Improving Security through E-Governance during Transition in Kosovo
Nehare Zeqiraj / Habit H. Hajredini (Pristina, Kosovo)

16:30-16:40 **Break**

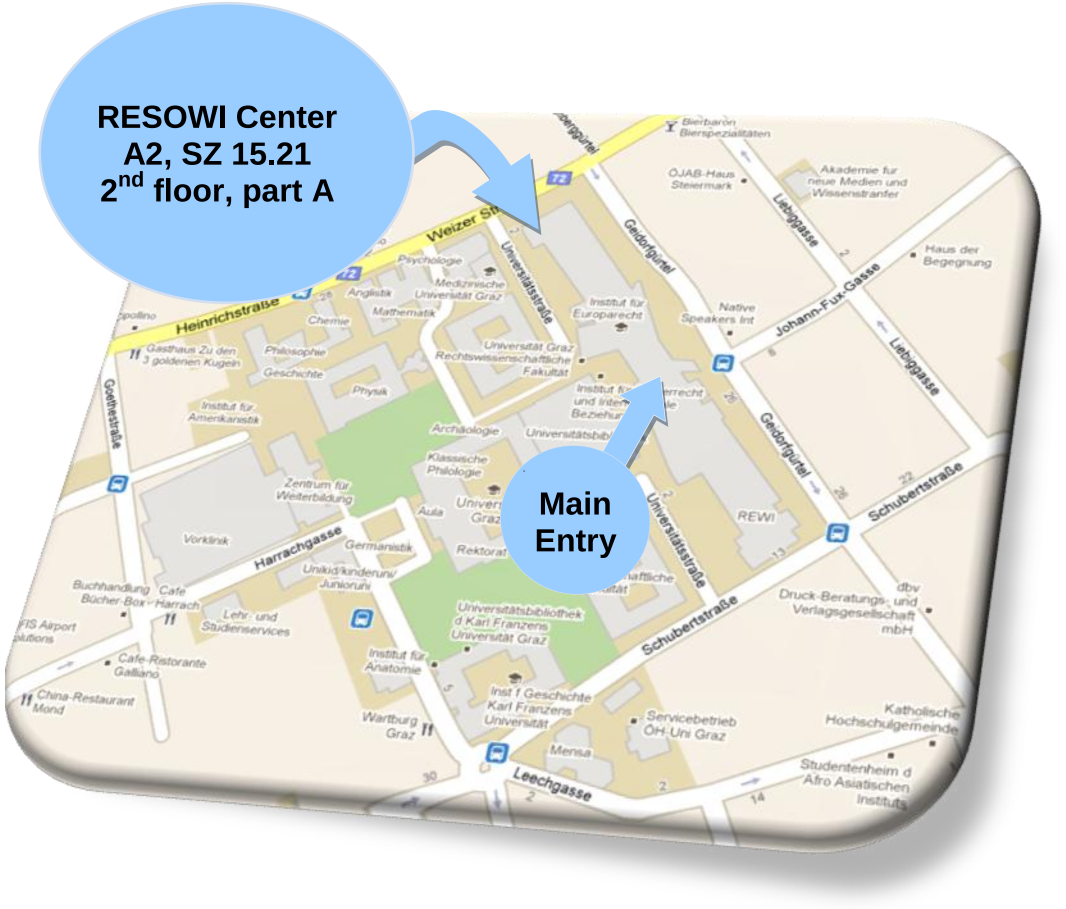
16:40-17:45 **High Level Discussion: The Future of Human Security in the Information Society – What Academia and Politicians Can Contribute**

Moderator: Matthias C. Kettemann (University of Graz)
Wolfgang Benedek (University / ETC Graz)
Gerhard Jandl (Foreign Ministry, Austria)
Wolfgang Slany (Technical University of Graz)
Jörg Leichtfried (European Parliament)

17:45-18:00 **Closing Remarks**
Wolfgang Benedek

18:00-19:00 **Closing Cocktail**

Conference Venue



RESOWI Center
A2, SZ 15.21
2nd floor, part A

Main
Entry

Organizing Committee

Wolfgang Benedek | Paul Gragl
Matthias C. Kettemann | Heike Montag
Cristina Pace | Pascoal Santos Pereira

Institute of International Law and International Relations
University of Graz

Universitätsstraße 15/A4, 8010 Graz, Austria
T | +43 316 380 3810
F | +43 316 380 9455
E | humansecurity@uni-graz.at
W | http://goo.gl/6GoMG

Human Rights @ Uni Graz

Learn all about our research, events and experts at **uni-graz.at/humanrights**

Partners

The **University of Graz** is one of the largest institutions of higher education in Austria. With more than 30,000 students and 3,800 employees, it makes an essential contribution to the vibrant life of the Styrian capital. Diversity and a wide scope characterize the education programmes at the six faculties. Students can choose from more than 100 bachelor, master and diploma programmes.

www.uni-graz.at

The **Institute of International Law and International Relations** is a centre of legal excellence that is committed to developing international law and the law of international organizations through cutting-edge research and innovative international legal teaching.

Since 2000 the Institute of International Law and International Relations of the University of Graz and the **European Training and Research Centre for Human Rights and Democracy (ETC)** Graz have developed a research and teaching focus on the concept of human security. By 2011 some ten security scholars of various academic backgrounds have founded the **Human Security Focus Group** to streamline their research, to promote the added value of human security, and to ensure that the human rights city Graz remains a centre of excellence for human security research, teaching and practice.

www.uni-graz.at/vrewww

University of Graz

Institute of International Law and International Relations

HUMAN SECURITY FOCUS GROUP

The **ETC** has been set up as a non-profit association and started its work in October 1999. Its main aim is to conduct research and training programs in the fields of human rights, democracy and the rule of law in close co-operation with the University of Graz. Special emphasis is put on training programs for civil servants, the police and the army.

www.etc-graz.at

The research group on **human rights** has grown into an important institution at the Faculty of Law of the University of Graz. It aims to link the faculty's research competences with regard to human rights, democracy and gender and to streamline international cooperation. Researchers focus specifically on human rights protection in Europe, human rights and human security, rule of law, asylum, migration and human rights and the protection against discrimination.

www.uni-graz.at/humanrights

The **SPBUILD: Sustainable Peace Building Research and Training Network** has been created under the Marie Curie Actions of the Seventh Framework Programme/People by a solid and dynamic network of European institutions of higher learning. It consists of a group of nine universities and one research centre with twelve years of collaborative experience under the aegis of EDEN – HumanitarianNet. These research partners have undertaken joint research, published, created and developed Research Masters and/or European Doctoral Programmes and have created a European Doctoral Enhancement Programme on Peace and Conflict Studies (EDEN) that offered annual international seminar-workshops for doctoral students leading towards a joint European Doctorate in Peace and Conflict Studies.

www.humanitariannet.deusto.es/SPBuild

The **Austrian Institute for International Affairs (oiip)** is an independent, non-profit think-tank based in Vienna. The oiip was the first institute in Austria to focus on globalization, European integration, comprehensive security, and the comparative study of international affairs. It advises on public policy, conducts primary scientific research, supports the international academic exchange, and plays an important role in second track-diplomacy. Members of the institute publish widely, are consulted by the government, and regularly feature in the media.

www.oiip.ac.at

The **Austrian National Defence Academy** is the highest military training and research institution in the Austrian Ministry of Defence and Sports (MoDS). In addition to conducting all courses from senior staff to strategic level, the Defence Academy is the prime think-tank within the MoDS for research in security, defence and military policy and strategy.

www.bmlv.gv.at

5th Graz Workshop on the Future of Security

Human Security in the Information Society: Regulating Risks – Empowering People

Friday, 16 March 2012 | University of Graz, Austria

RESOWI Center A2, SZ 15.21

Mehr menschliche Sicherheit im Internet

Was tun gegen ACTA, Cyberkriminalität und Menschenrechtsbedrohungen im Netz? Der 5. Grazer Workshop zur Zukunft der Sicherheit lieferte Antworten.

Matthias C. Kettemann

Der 5. Grazer Workshop zur Zukunft der Sicherheit thematisierte am 16.3. an der Rechtswissenschaftlichen Fakultät der Uni Graz die größten Herausforderungen des Internet für menschliche Sicherheit und Menschenrechte. Der erste Schritt: mehr Sensibilisierung, ein klareres Bekenntnis zum Menschenrechtsschutz und eine stärkere Zusammenarbeit von Staaten, Unternehmen und Individuen.

ACTA: eine nützliche Hysterie

"ACTA ist eine nützliche Hysterie" sagte Wolfgang Benedek vom Institut für Völkerrecht zu Beginn des 5. Grazer Workshops zur Zukunft des Internet. Denn nun rede man über Menschenrechte im Internet. Der Cyberspace, so Benedek, sei kein rechtsfreier Raum. Staaten, der private Sektor und Menschen müssten zusammenarbeiten, wobei Staaten die Hauptverantwortung in der Durchsetzung der Menschenrechte zukommt.

Gefahr der Gutgläubigkeit

"Wir sind alle viel zu schnell bereit, Informationen über uns herzugeben", sagte Wolfgang Slany vom Institut für Softwaretechnologie der TU Graz. "Die Menschen sind das schwächste Glied". Für wenig Geld könne man Software kaufen, um die Identität anderer User zu übernehmen. Slanys Lösung: mehr Datenbewusstsein und mehr Bewusstsein bei Computerunternehmen und Netzwerkadministratoren für die Sicherheitsprobleme, die sich aus sozialem Engineering ergeben. Ein erster Schritt: sich am Flughafen nicht über die Schulter lassen, wenn man surft, chattet und mailt.

Die 4. Generationen der Kriegsführung

“Das Internet dynamisiert die Kommunikation”, erklärte Ernst M. Felberbauer, und ermöglicht Kampagnen (wie “Kony 2012”) und Leaks (wie “Assad-Gate”). Dies beeinflusst auch die Wahrnehmung der 4. Generation der Kriegsführung, in der Staaten gegen nichtstaatliche Akteure wenden. Gleichzeitig hat der Arabische Frühling gezeigt, so der Leiter des Forschungsmanagements bei der Landesverteidigungsakademie, dass jene Regierungschefs der Welt, die nicht menschliche Sicherheit garantieren, ein Ablaufdatum hätten. In Österreich, so Felberbauer, werde zur Zeit eine Cybersecurity Strategie ausgearbeitet, die dem Schutz der Menschen im Internet dienen soll.

Eine ganze Generation wird illegalisiert

Um ACTA ging es natürlich auch: “Eine ganze Generation wird in Illegalität getrieben”, meint Jörg Leichtfried, Vorsitzender der österreichischen Delegation der SPÖ-Delegation im Europaparlament, während die Interessen großer Medienfirmen geschützt würden. Aber ACTA sei auch noch aus anderen Gründen problematisch: Das Strafrecht werde herangezogen, um Verletzung von Urheberrecht zu ahnden - und das sei falsch. Die Aktion gegen ACTA zeigte zum ersten Mal einen “Aufstand der Zivilgesellschaft” - und das sei beeindruckend. Nur weiter so, meinte Leichtfried in Bezug darauf, Europaparlamentarier unter Druck zu setzen, um menschenrechtliche Ziele zu erreichen. Das Internet könne so erfolgreich zur Mobilisierung der Zivilgesellschaft eingesetzt werden.

Mehr Kommunikation gefragt

Zentral meinte Wolfgang Slany, sei es aber, dass Menschenrechtsexperten und Techniker miteinander kommunizieren, um gemeinsam die Herausforderungen des Internet zu meistern. Auch das war Ziel und Ergebnis des Workshops.

Organisiert wurde der Workshop von Prof. Wolfgang Benedek und seinem Team vom Institut für Völkerrecht und Internationale Beziehungen in Kooperation mit dem Europäisches Trainings- und Forschungszentrum für Menschenrechte und Demokratie (ETC) Graz, der Landesverteidigungsakademie, dem Österreichisches Institut für Internationale Politik (OIIP) und der Marie Curie Action “Sustainable Peace Building” (7. EU-Rahmenprogramm).

Univ.-Ass. Mag. Dr. Matthias C. Kettemann, LL.M. (Harvard) arbeitet am Institut für Völkerrecht und Internationale Beziehungen der Karl-Franzens-Universität Graz und war Mitglied des Organisationskomitees des 5. Grazer Workshops zur Zukunft der Sicherheit. Kontakt: matthias.kettemann@uni-graz.at.

University of Graz
Institute of International Law
and International Relations

National Defence
Academy
Republic of Austria

UNIVERSITY OF GRAZ
EUROPEAN TRAINING & RESEARCH CENTER
FOR HUMAN RIGHTS AND DEMOCRACY

University of Graz
HUMAN SECURITY
FOCUS GROUP

5th Graz Workshop on the Future of Security

Human Security in the Information Society: Regulating Risks – Empowering People

16 March 2012 | University of Graz, Austria

Keynote Speakers

Wolfgang Benedek

Doctorate in law 1974, Master in Economics in 1976, studies abroad and practice in Paris (1976/77), Heidelberg (Max-Planck-Institute of Foreign Public Law and International Law 1979/80) and Vienna (International Legal Affairs Office of Foreign Ministry (1980-82); 1988 habilitation, since 1990 Professor at Institute of International Law and International Relations, University of Graz, Co-Director of the ETC.

Ernst M. Felberbauer

LtCol Ernst M. Felberbauer was trained as an infantry officer in the Austrian Armed Forces before earning a degree in Geography, Economics, English, Political Science and Contemporary History. He joined the National Defence Academy in Vienna in 1996. Since 2010, Mr. Felberbauer is Head of Research Management at the Austrian National Defence Academy. He is Austrian Representative to the ESDC Executive Academic Board and to the Steering Committee of the PfP Consortium of Defense Academies and Security Studies Institutes.

Jörg Leichtfried

Jörg Leichtfried studied law at the University of Graz from 1987 to 1994. In 2004, he moved in for the first time as an MEP in the European Parliament. In 2009 he was reelected for a second term. Furthermore, since 2009, Jörg Leichtfried is the Head of Delegation of the Social Democratic Party in the European Parliament.

Wolfgang Slany

Professor Wolfgang Slany is head of the Institute for Software Technology at Graz University of Technology. Until 2003 he studied and worked at Tokyo University and Vienna University of Technology. Slany's research areas include agile software development with usability engineering and knowledge management for large teams.

Human Security Focus

of the European Training and Research Centre for Human Rights and Democracy (ETC) Graz and the Institute of International Law and International Relations of the University of Graz

Since 2000, and in particular since 2003, a research, training and publication focus on human security has been developed at the ETC Graz and the Institute of International Law and International Relations of the University of Graz.

The research and training activities developed out of the support work completed for the Human Security Network of which Austria is a member and which had its ministerial conference under the Austrian chairmanship in Graz in 2003. The ETC also contributed actively to the drafting of the **Graz Declaration on Principles of Human Rights Education and Human Security** which was adopted by the conference. But already in 2000, the ETC had hosted a workshop on the relationship between human rights, human security and human development.

In 2003, the ETC elaborated a **Manual on Human Rights Education** with a particular focus on the relationship between human rights and human security, which has been translated into **15 languages**. Since that time the relationship between human rights and human security has been a focus of the work of the research teams both at the University of Graz and at the ETC Graz. The successful work is reflected in several publications (see below). Other areas of research include human security and international law, human security in post-conflict situations, human security and the prevention of terrorism, human security as personal security, human security and development etc.

I. The Human Security Team

A team of presently six scholars are actively involved in human security research. These are:

- **Wolfgang Benedek**, head of the Institute of International Law and International Relations, University of Graz and director of the ETC Graz
- **Gerd Oberleitner**, Institute of International Law and International Relations, University of Graz/ETC Graz
- **Veronika Apostolovski**, ETC Graz
- **Matthias C. Kettemann**, Institute of International Law and International Relations, University of Graz
- **Markus Möstl**, ETC Graz

II. Human Security Research

Presently, the human security focus is based on several projects, programmes and research components:

- a human security research component to the FP 6 project on "**Human Security in the Western Balkans**: The relationship between organised crime and terrorism and its effects on civil society and the state in the region (HUMSEC)" at the ETC Graz;
- the project: "**The Future of Security**: the influence of the concept of human security on international law and European security policy with special emphasis on the relationship between human security and human rights", supported by the research fund of the Austrian National Bank at the Institute of International Law ;
- the "**Student Exchange Programme in Human Security (SEPHS)**" which enjoys funding from the European Commission's Education, Audiovisual and Culture Executive Agency (EACEA) in the framework of the EU-CANADA Programme for Cooperation in Higher Education, Training and Youth;
- a contribution to the EU Cost 28 project on "**Human Security and Crises Management by EU**";
- the development of the third edition of the **Manual on Human Rights Education** (Wolfgang Benedek (ed.), Understanding Human Rights, Manual on Human Rights Education, 3rd ed., Neuer Wissenschaftlicher Verlag, Vienna, Intersentia, Antwerp, 2012);
- participation in **research programmes** of other institutions, such as a **UNESCO** investigation into the concept and implications of human security, to which Wolfgang Benedek contributed a study on human security and human rights;
- an assessment, in 2007, of the relevance of the concept of human security for the **OSCE** (Oberleitner);
- the participation, by the ETC, in the project "**Multi-stakeholder Partnerships in Post-Conflict Reconstruction: The Role of the European Union**" (MULTIPART). In the Multipart project consortium under the 7th Framework programme, the ETC had the main responsibility for drafting a part on human security as a framework of analysis for the research into multi-stakeholder partnerships in post-conflict situations.

III. Teaching and Training Activities

All these activities have led to a particular competence in the field of human security, which has been reflected in training programmes, in particular the yearly **Summer Academy on Human Security and Human Rights**, organised by the ETC 2003-2010. The ETC regularly publishes a peer-reviewed electronic journal called **Human Security Perspectives** and the **HUMSEC Journal**.

Professor Benedek und Dr. Oberleitner also contribute to the EU-funded European Regional Master Programme in Human Rights and Democratisation (EIUC Venice) by regularly teaching classes on human rights and human security, while Dr. Oberleitner also teaches human security at Science Po in Paris.

In the academic years 2008-2010 further teaching activities on human security were developed for the **Student Exchange Programme in Human Security (SEPHS)**, which created an opportunity for Canadian and European undergraduate students from six universities to deepen their knowledge and sensibility in the field of human security through a transatlantic mobility programme.

Since 2011, Prof. Benedek offers a yearly course on human security in international law and international relations at the University of Graz.

The research focus is developed further through past and ongoing diploma theses and doctoral dissertations:

- Hauthaler, Nathan, The Responsibility to Protect in International Law – A Shift in the Intervention Debate? (diploma thesis)
- Hussien, Mohammud A., Collective Intervention and Regional Enforcement Action in Africa: Challenges and Prospects of the AU System of Peace and Security (doctoral dissertation)
- Kopetz, Clemens, Die Anwendbarkeit von humanitärem Völkerrecht auf nicht-internationale Konflikte unter dem Gesichtspunkt der menschlichen Sicherheit (diploma thesis)
- Kettemann, Matthias C., Revisiting the Interposition of States Between Individuals and International Law (doctoral dissertation)
- Mamoucha, Sofia, Operationalising human security in terms of the European Security and Defense Policy: The case of EULEX Kosovo (Master thesis)
- Möstl, Markus, Das Konzept der menschlichen Sicherheit in der Europäischen Sicherheits- und Verteidigungspolitik (doctoral dissertation)
- Skasa Albin, Die Intervention von Drittstaaten im internen bewaffneten Konflikt und ihre Auswirkungen (diploma thesis)
- Jovanovic, Sinisa, Contemporary Law of Occupation. The Development of the Law of Occupation and the Obligation to Restore and Ensure “L’ordré et la Vie Public” with Special Reference to the Occupation of Iraq” (diploma thesis)
- Ablasser, Christine, Die völkerrechtlichen Maßnahmen zum Schutz von Frauen vor Gewalt in bewaffneten Konflikten (diploma thesis)
- Konrad, Corinna, The Human Security Concept of Japan (diploma thesis)
- Zwitter, Andrej, Prevention of Terrorism: A Human Security Approach (doctoral dissertation)

IV. Publications

- Benedek, Wolfgang, Markus Möstl, Matthias C. Kettemann, Mainstreaming Human Security: A Research Agenda, in: Benedek/Kettemann/Möstl (eds.), Mainstreaming Human Security in Peace Operations and Crisis Management. Policies, Problems, Potential, Routledge, London 2010, 1-11 (with Wolfgang Benedek und Markus Möstl).
- Benedek, Wolfgang, Markus Möstl, Matthias C. Kettemann, A Roadmap towards Mainstreaming Human Security, in: Benedek/Kettemann/Möstl (eds.), Mainstreaming Human Security in Peace Operations and Crisis Management. Policies, Problems, Potential, Routledge, London 2010, 245-257 (with Wolfgang Benedek und Markus Möstl)
- Benedek, Wolfgang, The Human Security Approach to Terrorism and Organized Crime in Post-Conflict Situations, in: Wolfgang Benedek, Christopher Daase, Vojin Dimitrijevic, Petrus van Duyne (eds.), Transnational Terrorism, Organized Crime and Peace Building. Human Security in the Western Balkans, Palgrave Macmillan, Great Britain 2010, 3-16.
- Benedek, Wolfgang, Mainstreaming human security in United Nations and European Union peace and crises management operations: policies and practice, in: Wolfgang Benedek/Matthias C. Kettemann/Markus Möstl (eds.), Mainstreaming Human Security in

Peace Operations and Crises Management. Policies, Problems, Potential, London/New York, Routledge, 2010, 13-31.

- Benedek, Wolfgang, The Role of Education for Sustainable Peace-Building, in: Ernst M. Felberbauer, Predrag Jurekovic and Frederic Labarre (Eds.), Supporting Bosnia and Herzegovina, The Challenge of Reaching Self-Sustainability in a Post-War Environment, National Defense Academy, Vienna 2009, 183-204.
- Benedek, Wolfgang and Kettemann, Matthias C., Menschliche Sicherheit und Menschenrechte, in Claudia Ulbert/Sascha Werthes (eds.), Menschliche Sicherheit. Globale Herausforderungen und regionale Perspektiven, Nomos, Baden-Baden 2008, 94-109.
- Benedek, Wolfgang, Human Security and Human Rights Interaction, in: Moufida Goucha and John Crowley (eds.), Rethinking Human Security, International Social Science Journal 2008, 7-17.
- Benedek, Wolfgang, Die Relevanz des Konzepts der menschlichen Sicherheit für die persönliche Sicherheit, in: Martin H. W. Möllers/Robert Chr. Van Ooyen (eds.), Jahrbuch Öffentliche Sicherheit 2006/2007, Verlag für Polizeiwissenschaft, Clemens Lorei, Frankfurt, 2007, 519-533.
- Benedek, Wolfgang, Human Rights and Human Security: Challenges and Prospects, in: Alice Yotopoulos-Marangopoulos (ed.), L'Etat Actuel des Droits de l'Homme dans le Monde, Defis et Perspectives, Conférence internationale à l'occasion du 25^{e} anniversaire d'activités de la FMDH, Editions A Pedone, Paris, 2006, 97-110.
- Benedek, Wolfgang, Der Beitrag des Konzeptes der menschlichen Sicherheit zur Friedenssicherung, in: Klaus Dicke, Stephan Hobe, Karl-Ulrich Meyn, Anne Peters, Eibe Riedel, Hans-Joachim Schütz and Christian Tietje (eds.), Weltinnenrecht, Liber amicorum Jost Delbrück, Duncker & Humblot, Berlin 2005, 25-36.
- Benedek, Wolfgang, Human Security and Prevention of Terrorism, in: Wolfgang Benedek and Alice Yotopoulos-Marangopoulos (eds.), Anti-Terrorist Measures and Human Rights, Martinus Nijhoff Publishers, Leiden/Boston, 2004), 171-184.

- Kettemann, Matthias C., Regimewechsel und Schutzverantwortung: Völkerrechtliche Aspekte des Libyen-Konfliktes [Regime Change and Responsibility to Protect, International Legal Aspects of the Conflict in Libya], in: Otto Kammerlander (ed.), Expertenforum SpringerRecht.at 2011, Wien/New York, Springer 2012, 125-129.
- Kettemann, Matthias C., Lessons from Libya: a Test Case for Human Security Mainstreaming?, Human Security Perspectives 1/2011, 40-52.
- Kettemann, Matthias C., Regimewechsel und Schutzverantwortung: Völkerrechtliche Aspekte des Libyen-Konfliktes [Regime Change and Responsibility to Protect: International Legal Aspects of the Conflict in Libya], SpringerRecht.at Expertenforum, 17 May 2011, http://www.springerrecht.at/regimewechsel-und-schutzverantwortung-volkerrechtliche-aspekte-des-libyen-konfliktes_matthias-c-kettemann.
- Kettemann, Matthias C., UN-Sicherheitsrat beruft sich in Libyen-Resolutionen erstmals auf Responsibility to Protect [UN Security Council, for the first time, refers to Responsibility to Protect in his Libya Resolutions], BOFAX 377D, http://www. ruhr-uni-bochum.de/ifhv/documents/bofaxe/bofaxe2011/377d.pdf.
- Kettemann Matthias C., Menschliche Sicherheit: Erfolgsrezept für Friedensoperationen von UNO und EU [Human Security: Formula for Success for UN and EU Peace Operations], Global View 4/2010.
- Kettemann Matthias C./Markus Möstl, Die Bedeutung menschlicher Sicherheit [The Meaning of Human Security], Global View 1/2009, 10.
- Kettemann Matthias C., Markus Möstl, Der Königsweg zur Verbindung von Menschenrechten und Sicherheit: der Beitrag des Konzeptes menschlicher Sicherheit

zur Friedenskultur [How to Best Unite Human Rights and Security: The Contribution of the Concept of Human Security to a Culture of Peace], in: Bettina Gruber und Werner Wintersteiner (eds.), Menschenrecht und Frieden. Jahrbuch Friedenskultur 2009, Klagenfurt, Drava Verlag, 2009, 110-123.

- Kettemann, Matthias C., Harmonizing International Constitutional Law and Security: the Contribution of the Concept of Human Security, in: Harald Eberhard/Konrad Lachmayer/Gregor Ribarov/Gerhard Thallinger (eds.), Constitutional Limits to Security. Proceedings of the 4th Vienna Workshop on International Constitutional Law, Wien/Baden-Baden 2009, 109-134.
- Kettemann, Matthias C., The Visiting Practice of the European Committee for the Prevention of Torture as an Instrument to Further Human Security, Human Security Journal/Révue de la Sécurité Humaine (2007) 3, 79-88 (with Antonia Dürnsteiner).
- Kettemann, Matthias C., „The Conceptual Debate on Human Security and its Relevance for the Development of International Law“, Human Security Perspectives 3 (2006) 1, 39-52.

- Kicker Renate/Standard-setting through Monitoring? The Role of selected Council of Europe Expert Bodies for the Development of the European Rights Order, Council of Europe Publishing, forthcoming 2012

- Möstl, Markus, Monitoring Human Rights by Council of Europe Bodies: Quo vadis?, in: European Yearbook on Human Rights, Vol. 4., 2012, 303-312.
- Möstl, Markus, Civil-military coordination in the Common Defence Policy of the European Union, in: Human Security Perspectives 1/2011, pp.30-39.
- Möstl, Markus, Reforming the Council of Europe’s human rights monitoring mechanisms, in: Netherlands Quarterly of Human Rights, Vol. 4/2011, (with Renate Kicker and Emma Lantschner)
- Möstl, Markus, Assessing the impact of multi-stakeholder partnerships for human security, in: Owen Greene, Andrea De Guttry and Wolfgang Benedek (eds.), Peace-building and human security after conflict: multi-stakeholder partnerships. New York/London, Routledge, (forthcoming 2012).
- Möstl, Markus, MultiPart country study on Kosovo, available online at: www.multi-part.eu, 2010 (with Wolfgang Benedek and Jens Narten).
- Möstl, Markus, Core tasks of good governance and their impact on peacebuilding and human security, in: MultiPart thematic paper on multi-stakeholder partnerships active in the field of good governance, democracy and rule of law, available online at: www.multi-part.eu, 2010, 53-79.
- Möstl, Markus, Overall conclusions, in: MultiPart thematic paper on multi-stakeholder partnerships active in the field of good governance, democracy and rule of law, available online at: www.multi-part.eu, 2010, 226-236.Mainstreaming human rights in the Common Security and Defence Policy: reality or catchphrase? in: European Yearbook on Human Rights, Vol. 2., 2010, 247-262.
- Möstl, Markus, The European way of promoting human security in crisis management operations: A critical stocktaking, in: Wolfgang Benedek, Matthias C. Kettemann and Markus Möstl (eds.), Mainstreaming human security in peace operations and crisis management. Policies, problems, potential. New York/London, Routledge, 2010, 141-158.
- Möstl, Markus, “Human Security and the European Security and Defence Policy: Achievements and Challenges”, in: Ferrándiz Francisco (ed.), Multidisciplinary Perspectives on Peace and Conflict: A View from Europe, Humanitarian Net Publication, Universidad de Deusto, Spain (2009).

- Möstl, Markus, Das Konzept der Menschlichen Sicherheit in der Europäischen Sicherheits- und Verteidigungspolitik, in: Erstausgabe Vol. 2, 2009, 181-188.

- Oberleitner, Gerd, Human Security, in David P. Forsythe, Encyclopedia of Human Rights (Oxford: Oxford University Press), forthcoming 2009.
- Oberleitner, Gerd, Responsibility as Security to Protect, Nuntium, forthcoming 2009.
- Oberleitner, Gerd, The OSCE and Human Security, Security and Human Rights 1 (2008), 382-390.
- Oberleitner, Gerd, "Porcupines in Love: The Intricate Convergence of Human Rights and Human Security", European Human Rights Law Review 6 (2006), 588-606.
- Oberleitner, Gerd, "Human Security – A Challenge to International Law?", Global Governance 11 (2005) 2, 185-203.
- Oberleitner, Gerd, "A *Just War* against Terrorism?", Peace Review 16 (2004) 3, 263-268.
- Oberleitner, Gerd, "Human Security and Human Rights," European Training and Research Centre for Human Rights and Democracy Occasional Paper No. 8 (2002), http://www.etc-graz.at/publikationen/Human%20Security%20occasional%20paper.pdf.
- Oberleitner, Gerd, "Civil Rights Sacrificed on Altar of Security", Times Higher Education Supplement 22, 6 December 2002 (with Conor Gearty).

INSTITUTE OF INTERNATIONAL LAW AND INTERNATIONAL RELATIONS

Focal Point on Internet Governance and Human Rights

Univ.-Prof. Mag. Dr. Wolfgang Benedek | Mag. Dr. Matthias C. Kettemann, LL.M. (Harvard)

Focal Point on Internet Governance and Human Rights

Background | Team | Activities | Publications

As technologies change, so must law. The digital revolution caused by the evolution of information and communication technologies (ICTs) has given birth to a new field of law: the law of the information society. The Internet, as a network of networks that ICTs have dynamized, is regulated through a process of Internet Governance. In both the law of the information society and that of Internet Governance, human rights play a central role.

The Institute of International Law and International Relations of the University of Graz, Austria, has a strong tradition of innovative research and teaching and a convincing track record of covering emerging issues of international law. Since 2001, the Institute has committed resources specifically to the international normative instruments regulating the evolving international information order.

While other institutes of the Law Faculty of the University of Graz focus on subjects as European legal development and ICTs, civil law and ICTs, intellectual property and ICT and cybercrime, the Institute of International Law and International Relations broaches more fundamental issues: How can (and how should) the Internet be ruled in a way that is both effective and sensitive to human rights?

Research on this far-reaching question has been conducted by Professor Wolfgang Benedek, head of the Institute of International Law and International Relations, and a team of young researchers in the framework of three projects funded by the Austrian Science Fund. The projects have led to five workshops, numerous publications, including two books, and have enabled the researchers from Graz to reach an established position in the international research community, namely with regard to human rights in the information society.

Wolfgang Benedek and the members of the Focal Point have been present and active during the most important moments of the evolution of the information society in the last seven years: from the WSIS process and selected ICANN International Public Meetings to all Internet Governance Forums held until today.

Members of the Focal Point are further active in several Dynamic Coalitions, including those committed to furthering human rights, and the freedom of expression, on the Internet. Focal point members Professor Wolfgang Benedek and Matthias C. Kettemann are also members of the Global Internet Governance Academic Network

(GigaNet) and contributors to its workshops. Both publish widely on Internet Governance and human rights, both offline and online.

I. The team of the focal point

Presently, a team of two scholars is actively involved in research on the legal dimensions of the information society:

Professor Dr. Wolfgang Benedek

head of the Institute of International Law and International Relations, University of Graz; director of the European Training and Research Centre for Human Rights and Democracy (ETC) of the University of Graz; member of the Global Internet Governance Academic Network, the Internet Rights and Principles Coalition and the Civil Society Internet Governance Caucus

Dr. Matthias C. Kettemann, LL.M. (Harvard)

research fellow and lecturer, Institute of International Law and International Relations, University of Graz; Co-Chair of the Internet Rights and Principles Coalition; blogs on international law and the Internet at http://internationallawandtheinternet.blogspot.co.at; writes regularly on Internet and human rights for online and offline audiences; reviewer for contributions related to the information society for *Political Communication, First Monday*, *Masaryk Journal of Law and Technology* and *Global Information Society*; member of the Global Internet Governance Academic Network, the Dynamic Working Coalition on Internet Governance Mapping, the Internet Rights and Principles Coalition and the Civil Society Internet Governance Caucus

II. Projects and key activities on Internet Governance law

2012

- Wolfgang Benedek selected as expert for the Council of Europe Committee of Experts on Rights of Internet Users (MC-DUI)
- Council of Europe charges Wolfgang Benedek, Matthias C. Kettemann and Paul Gragl with providing a human rights assessment of new gTLDs
- Matthias C. Ketteman named thematic lead of the 5th initiative on human rights and the Internet of the Internet&Society Co:llaboratory
- Wolfgang Benedek named co-rapporteur by the Asia Europe Foundation for the 2012 Annual Informal EU/ASEAN Human Rights Workshop

2011

- Together with a team of scholars, Wolfgang Benedek developed the Charter on Internet Rights and Principles for the Internet Rights and Principles Coalition
- Matthias C. Kettemann named Co-Chair of the Internet Rights and Principles Coalition

2010

- Council of Europe contracts Wolfgang Benedek and Matthias C. Kettemann with writing a book on freedom of expression on the Internet

2005-2008

- We, the Information Society? The Role of Multi-Stakeholder-Participation for the Implementation of Human Rights Approaches (project leader: *Wolfgang Benedek*; research fellows: *Matthias C. Kettemann* (2006-2008)/*Veronika Bauer* (2006-2007)/*Catrin Pekari* (2005-2006))

2003-2005

- Human Rights in the Information Society (Project leader: *Wolfgang Benedek*; research fellow: *Catrin Pekari*)

2001-2003

- ICANN, OECD and WTO in the evolving international regulatory regime of the Internet (Project leader: *Wolfgang Benedek*; research fellow: Cat*rin Pekari*)

III. Teaching and training activities

- Units on human rights and the Internet at the annual Internet Governance Summer School in Meißen (*Wolfgang Benedek)*
- Austria’s first seminar on International Law and the Internet (*Matthias C. Kettemann*)
- Co-teaching a course on human rights aspects of IT for students of all faculties (*Matthias C. Kettemann*)
- Brown Bag Lunches on human rights and Internet law for students and the public (*Matthias C. Kettemann*)
- Unit on the law of the information society in the general course on international law (*Wolfgang Benedek*)

- Units on human rights aspects of the information society in the “Human Rights Debate Club” (*Wolfgang Benedek/Matthias C. Kettemann*)
- “Debate Club on Legal Questions of the Information Society” (*Wolfgang Benedek/Matthias C. Kettemann*)
- Workshops for teachers on the dangers and opportunities for children on the Internet
- Regular lectures for highs school students on the right to privacy on the Internet

IV. Publications

Books

- *Kettemann*, The Future of Individuals in International Law. Lessons from International Internet Law, Utrecht 2012 [in preparation].

- *Benedek*/*Kettemann*, Freedom of Expression on the Internet, Council of Europe, Strasbourg 2012 [in preparation].

- *Gahren/Haselbeck/Kettemann/Klug/Senges* (eds.), Menschenrechte und Internet. Zugang, Freiheit, Kontrolle [Human Rights and the Internet. Access, Freedom, Control]. Final Report of the 5th Initiative of the Internet&Society Co:llaboratory (Berlin: Internet&Society Co:llaboratory, 2012).

- *Benedek*, Wolfgang/Bauer, Veronika and Kettemann, Matthias C. (eds.), Internet Governance and the Information Society. Global Perspectives and European Dimensions (Utrecht: Eleven Publishing, 2008).

- *Benedek*, Wolfgang/Pekari, Catrin (eds.), Menschenrechte in der Informationsgesellschaft [Human Rights in the Information Society] (Hannover: Boorberg, 2007).

Recent Articles

2012

- *Kettemann*, Grotius goes Google: Der Einfluss der Internet Governance auf das Völkergewohnheitsrecht [Grotius goes Google: The Influence of Internet Governance on Customary International Law], in Christoph Vedder (ed.), Tagungsband 37. Österreichischer Völkerrechtstag 2012 [Collected Contributions to the 37th Annual Austrian Conference on International Law 2012], Vienna 2013 [in print].

- *Kettemann*, Internet Governance, in Elisabeth Staudegger (ed.), Informatikrecht [Law of Informatics], Springer Wien/New York 2012 [in print].

- *Kettemann*, Das Internet als internationales Schutzgut: Ließ der Arabische Frühling das Internetvölkerrecht erblühen? [The Arab Spring and International Internet Law: Does the Internet Enjoy International Protection?], ZaöRV, 3 (2012) [in print].

- *Kettemann*, Are Internet Governance Principles the New Pathway to Human Security and Human Rights Online?, Human Security Perspectives 1/2012 [in print].

- *Kettemann*, Menschenrechte als Maßstab für die Zukunft des Internet [Human Rights as the Normative Standard for the Future of the Internet], Springer Recht.at Expertenforum, http://www.jusportal.at/menschenrechte-als-masstab-fur-die-zukunft-des-internet_matthias-c-kettemann (2012).

- *Kettemann*, Wo soll Vint Cerf sein Pferd unterstellen? Zur Debatte um das Recht auf Internet-Zugang [Where should Vint Cerf put his horse? On the debate on the right to Internet access], juridikum (2012), 2, 13-15.

- *Kettemann*, Internet und Menschenrechte. Eine Ansage [Internet and Human Rights. A Call to Action], in Gahren/Haselbeck/Kettemann/Klug/Senges (eds.), Human Rights and the Internet. Access, Freedom, Control. Final Report of the 5th Initiative of the Internet&Society Co:llaboratory (Berlin: Internet&Society Co:llaboratory, 2012), http://cobase.collaboratory.de/w/Abschlussbericht_Menschenrechte_und_Internet, 21-25.

- *Kettemann*, Gibt es Schutzlücken im Internet? [Are there Human Rights Gaps on the Internet?] in Gahren/Haselbeck/Kettemann/Klug/Senges (eds.), Human Rights and the Internet. Access, Freedom, Control. Final Report of the 5th Initiative of the Internet&Society Co:llaboratory (Berlin: Internet&Society Co:llaboratory, 2012), http://cobase.collaboratory.de/w/Abschlussbericht_Menschenrechte_und_Internet, 26-34.

- *Kettemann*, The Power of Principles: Reassessing the Internet Governance Principle Hype, in: Erich Schweighofer/Franz Kummer/Walter Hötzendorfer (eds.), Transformation jurstischer Sprachen [Transformation of Legal Languages]. Tagungsband des 15. Internationalen Rechtsinformatik Symposions IRIS 2012 [Proceedings of the 15th International Legal Informatics Symposion], Vienna 2011, 445-448 (also published as: *Kettemann*, The Power of Principles: Reassessing the Internet Governance Principle Hype: Jusletter IT, 29.2.2012, www.jusletter-it.eu).

- *Kettemann*, Endlich bestätigt: Menschenrechte gelten online wie offline [Finally Resolved: Human Rights are Binding Offline Just as Online], jusPortal.at (Verlag Österreich), 24 July 2012, http://www.jusportal.at/endlich-bestatigt-menschenrechte-gelten-online-wie-offline_matthias-c-kettemann.

- *Kettemann*, UN Human Rights Council Confirms that Human Rights Apply to the Internet, EJIL Talk, 23 July 2012, http://www.ejiltalk.org/un-human-rights-council-confirms-that-human-rights-apply-to-the-internet/#more-5207.

- *Kettemann*, Die Stellschrauben des internationalen Rechts zur Durchsetzung der Internetfreiheit [The Adjustable Screws of International Law to Ensure Internet Freedom], Comment on Rolf H. Weber, Gibt es Grenzen für staatliche Beschränkungen der Internetfreiheit? [Are there Limits to State Policies Limiting Internet Freedom], MIND (Multistakeholder Internet Dialogue) # 3, Co:llaboratory Discussion Paper Series No. 1, May 2012, 72-77, http://dl.collaborato ry.de/mind/mind_03.pdf.

- *Kettemann*, Ensuring Global Development through Internet Freedom, In Focus, Digital Rights Watch, 24 April 2012, http://digitalrightswatch.org/ ?p=105250.

2011

- *Benedek*, Wolfgang, Multistakeholder Governance als politisch-rechtliche Innovation, in: MIND – Multistakeholder Internet Dialog, Co:llaboratory Discussion Paper Series No. 1, Wolfgang Kleinwächter (Hg.), Berlin, Mai 2011, 21-22.

- *Benedek*, Wolfgang, The Relevance of the Multi-Stakeholder Approach and Multi-Track Diplomacy for Human Rights Diplomacy, in: Michael O’Flaherty/Zdzislaw Kedzia/Amrei Müller/George Ulrich, Human Rights Diplomacy: Contemporary Perspectives, Martinus Nijhoff Publishers, Leiden/Boston, 2011, 251-261.

- *Kettemann,* Nationale Sicherheit und Informationsfreiheit [National Security and Freedom of Information], in Kirsten Schmalenbach (ed.), Tagungsband Österreichischer Völkerrechtstag 2011 [Collected Contributions to the 36th Annual Austrian Conference on International Law 2011], Vienna 2012 [in print].

- *Kettemann*, Building the Legal Framework of the Information Society: Lessons from Combating Hate Speech, in: Erich Schweighofer/Frank Kummer (eds.), Europäische Projektkultur als Beitrag zur Rationalisierung des Rechts. Tagungsband des 14. Internationalen Rechtsinformatik Symposiums IRIS 2011 [European Project Culture as a Contribution to the Rationalization of Law. Contributions to the 14th International Symposium on Legal Informatics] , ÖCG, Vienna 2011, 179-182 (also published as *Kettemann*, Building the Legal Framework of the Information Society: Lessons from Combating Hate Speech, in: Jusletter IT, 24 February 2011, www.jusletter-it.eu).

- *Kettemann,* Wider die Cyberutopie in der Weltpolitik. Twitter und Facebook machen noch keine Revolution [A Critique of Cyber Utopism in Global Politics. Revolutions Need More than Twitter and Facebook], juridikum (2011), 2, 155-158.

- *Kettemann*, Recht und Macht im Internet. Onlinehegemonien und ihre Durchbrechungen [Law and Power in the Internet: Online Hegemonies and their Transcendence], juridikum 4/2011, 457-459 (and coordination of the thematic focus on the juridikum on law and power on the Internet).

- *Kettemann*, Ensuring Human Rights Online: An Appraisal of Selected Council of Europe Initiatives in the Information Society Sector in 2010, in W. Benedek et al. (eds.), European Yearbook on Human Rights 2011, Vienna 2011, 461-482.

2008-2010

- *Benedek/Kettemann*, The Council of Europe and the Information Society, in Renate Kicker (ed.), The Council of Europe: Pioneer and Guarantor for Human Rights and Democracy, Strasbourg 2010, 88-93.

- *Kettemann*, Internet Governance and Human Rights in Europe, in: Wolfgang Benedek/Florence Benoît-Rohmer/Wolram Karl/Manfred Nowak (eds.), European Yearbook on Human Rights 2010, Neuer Wissenschaftlicher Verlag, Vienna 2010, 335-352.

- *Kettemann*, Taking Sexting Seriously: Should Europe Start Prosecuting "Sexters", juridikum (2010) 4, 402-413.

- *Kettemann*, Reform statt Revolution: ICANNs neues Accountability-Regime im Lichte europäischer Kritik [Reform, Not Revolution: The Accountability Regime of ICANN in Light of European Critique], jusIT (2009) 6, 215-220.

- *Kettemann*, Der Europarat und die Informationsgesellschaft [The Council of Europe and Information Society], politicum (2009) 108, 103-108 (with Wolfgang Benedek).

- Bauer, Veronika, Regionalizing E-Inclusion: Approaches of the EU and Austria, in Benedek, Wolfgang/Bauer, Veronika/Kettemann, Matthias C. (Hrsg.), Internet Governance and the Information Society. Global Perspectives and European Dimensions (Utrecht: Eleven Publishing, 2008), 115-125.

- *Bauer, Veronika/Kettemann, Matthias C.,* Internet Governance, Quo Vadis? Meeting the Challenges of Internet Governance in a Multi-Stakeholder Environment, in Benedek, Wolfgang/Bauer, Veronika/Kettemann, Matthias C. (eds.), Internet Governance and the Information Society. Global Perspectives and European Dimensions (Utrecht: Eleven Publishing, 2008),163-171.

- *Benedek*, Wolfgang/Kettemann, Matthias C./Senges, Max, The Humanization of Internet Governance: A Roadmap Towards a Comprehensive Global (Human) Rights Architecture for the Internet, http://giganet.igloogroups.org/annualsymp (2008).

- *Benedek*, Wolfgang, Der Schutz der Meinungsäußerungs- und Medienfreiheit in der Informationsgesellschaft [The protection of the freedom of expression and of the media], in Benedek, Wolfgang/Pekari, Catrin (eds.), Menschenrechte in der Informationsgesellschaft [Human Rights in the Information Society] (Hannover: Boorberg, 2007), 125-146.

- *Bauer, Veronika/Kettemann, Matthias C.,* Safeguarding the Commons in (and of) the Information Society: How Internet Governance Can Help Avoiding the Real 'Tragedy of the Commons', Re-public: re-imagining democracy (2007), http://www.re-public.gr/en/?p=101.

- *Bauer, Vernonika/Kettemann, Matthias C.,* Menschenrechtliche Implikationen der Informationsgesellschaft und österreichische Regulierungsansätze [Human Rights Implications of the Information Society and Austrian Regulatory

Approaches], in Benedek, Wolfgang/Pekari, Catrin (eds.), Menschenrechte in der Informationsgesellschaft [Human Rights in the Information Society] (Hannover: Boorberg, 2007), 293-323.

- *Benedek, Wolfgang,* Internet Governance and Human Rights, in Benedek, Wolfgang/Bauer, Veronika/Kettemann, Matthias C. (eds.), Internet Governance and the Information Society. Global Perspectives and European Dimensions (Utrecht: Eleven Publishing, 2008), 31-49.

- *Kettemann, Matthias C.,* ICANN und Internet Governance: Aktuelles zur Suche nach Patentrezepten gegen Legitimationsdefizite [ICANN and Internet Governance: Recent Developments in the Search for More Legitimacy], jusIT (2008) 5, 165-168.

- *Kettemann*, Matthias C., E-Inclusion as a Means to Bridge the Digital Divides: Conceptual Issues and International Approaches, in Benedek, Wolfgang/Bauer, Veronika/Kettemann, Matthias C. (eds.), Internet Governance and the Information Society. Global Perspectives and European Dimensions (Utrecht: Eleven Publishing, 2008), 51-61.

V. Contacting the Focal Point

Professor Dr. Wolfgang Benedek

Institute of International Law and International Relations
University of Graz
Universitätsstraße 15/A4
8010 Graz, Austria

Tel: +43/316/380-3411
Fax: +43/316/380-9455
Mail: wolfgang.benedek@uni-graz.at

Website: http://www.uni-graz.at/vrewww

Dr. Matthias C. Kettemann, LL.M. (Harvard)

Institute of International Law and International Relations
University of Graz
Universitätsstraße 15/A4
8010 Graz, Austria

Tel: +43/316/380-6711
Fax: +43/316/380-9455
Mail: matthias.kettemann@uni-graz.at

Blog: http://internationallawandtheinternet.blogspot.co.at