International Seminars on Planetary Emergencies
44th Session
Erice – August 22, 2011

The Role of Science in Information Technologies and Internet Tools in Developing Countries

Cyber Repression: Going Worse. What can be done?

Henning Wegener

The World Federation established its Permanent Monitoring Panel on Information Security exactly ten years ago, impressed by the growing damage potential looming in cyberspace. These dangers were already very real at that time, but in view of the *current*, civilization-threatening dimension of the cyber threat and the over-riding role cyber issues are taking in concerned public debate, those PMP members of the first hour can almost be credited with a sense of premonition. More than before, we are today facing a truly planetary emergency. It affects developing countries no less than others.

The Panel, one of the first groups in civil society world-wide to take a multi-disciplinary approach to the cyber issue, has tried from the beginning, in the best tradition of Erice, to develop a comprehensive analysis and strategy for harnessing the threats in cyberspace, as is evident from the title of its first major document, "Toward a Universal Order of Cyberspace", and, throughout the last decade has concentrated on key issues of cyber security, especially cyberwar, cyberterrorism, and cyber conflict in general. Our analysis and recommendations have increasingly crystallized around the concepts of cyber stability and cyber peace, as evidenced by the Erice Declaration of 2009, and our latest publication, "The Quest for Cyber Peace", co-authored by the Secretary General of ITU[1].

One important focus of our work has been the steady growth of massive Government interference in the freedom of digital information by censorship in the Internet, in violation of International Law[2], - and in contradiction with the sacred tenets of Erice where we have always defended the free flow of information as a prerequisite of civilized society[3]. The

[1] www.itu.int/pub/S-GEN-WFS.01-1-2011

[2] In particular, in the Universal Declaration of Human Rights ("UDHR"), the International Covenant on Civil and Political Rights ("ICCPR") and the International Covenant on Economic, Social and Cultural Rights ("ICESCR") protect the right of anybody to receive and impart information of all types, regardless of frontiers and through any chosen medium.

[3] "All governments should make every effort to reduce or eliminate restrictions on the free

consequences of comprehensive censorship – cyber repression - are grave and cannot be overestimated. Citizens are cut off from important benefits of the information age, and receive a skewed view of world reality, condemning them to political immaturity. Massive cyber repression can alter the collective state of mind of a nation. The gravity of massive information suppression is at par with other variants of cyber crime and cyber conflict und thus rightly in the purview of our work. Moreover, cyber repression hits hardest in developing countries which tend to have less elaborate legal and judicial systems, and where authoritarian structures are more widely spread and more persistent. Developing countries would be the greatest beneficiaries of the free acquisition of knowledge and free access to communication. Our work on cyber repression thus fits particularly well within the general theme of this session.

All governments need to have an eye on Internet contents for reasons of *ordre public*. There must be control to cut out child

flow of information, ideas and people'' Erice Statement 1982. ''All governments should recognize that international law guarantees the free flow of information and ideas; these guarantees also apply to cyberspace. Restrictions should be as necessary and accompanied by a process for legal review'' Erice Statement on Principles for Cyber Stability and Cyber Peace, 2009 pornography, violation of intellectual property rights, incitation to crime, racial hatred and anarchy. But in our earlier work we have been precise in providing a yardstick for alleviating the tension between freedom of expression and illegal repression. The criteria is the existence of clear legal prescription, respecting the International Covenants of Human Rights and Freedom of Expression, and access to independent legal review. Cyber Repression, as used in this presentation, lacks these essential prerequisites. No further definition is needed in this context. Cyber repression is by no means the preserve of developing countries that have inadequate democratic credentials. Many other countries are far from innocent.

The PMP has gone public with its indictment of cyber repression three times in the last years. At the 2005 session of the World Summit on the Information Society we submitted a document "Information Security in the Context of the Digital Divide[4]". Some of its recommendations are directed at the "Denial of information access through Internet filtering". The case against cyber repression has again been made in a book we published jointly with the EastWest Institute in 2010[5]. Finally, this mode of infringement of information access and information integrity is also featured in

[4] Document WSIS-05/TUNIS/CONTR/01-E

[5] www.ewi.info

"The Quest for Cyber Peace", where it is clearly indicated that cyber repression is incompatible with cyber peace[6].

If I undertake today to revisit the problem, there are alarming reasons to do so. Especially in the last two years the situation world-wide has deteriorated both quantitatively and qualitatively. That must spur our analysis, but also our thinking in action terms; our former operative recommendations must be strengthened.

One reason for the rapid, substantial worsening of the situation is the growth process in digital technologies; another is the recent emergence and phenomenal growth of the "new social networks". Since we first worked on the topic in 2004, the number of computers world-wide has more than doubled, and access to the Internet via broad band has grown even more steeply. There are now billions of mobile devices, especially in developing countries, increasingly on-line capable; at the same time, fixed and mobile technologies converge. The advent of the mobile Internet and interactive Web 2.0 options increasingly permeate the developing world as well.

At least since 2010, the New Media have firmly established their role, together with the Internet and mobile phones, as novel and

[6] All PMP documents are also available at its website www.unibw.de/infosecur

mighty mobilization and news transmission tools. The new networks, were initially designed for "social" purposes, to allow people networking and social interaction. But in the process they have developed unprecedented group dynamics, beyond mere communication and knowledge acquisition. The figures are astounding. By May 2011, Facebook had 600 million (!) members who communicate in 70 languages, helped by 50.000 servers. Twitter users now number close to 200 million (175 by September 2010) who emit corresponding millions of "tweets". YouTube receives an average of 2 billion (!) visits daily (in exceptional moments up to 7 billion). The result is a true explosion of the numbers of stakeholders in the information process, and of the potential for collective action[7].

I do not intend to join the current lively debate about to which extent these new processes, and especially the new social networks, have contributed to the current Middle Eastern revolutions, starting with the 2009 Iranian unrest. Some see the networks as the new "liberators", novel tools of democratization, profoundly reshaping our political processes and their instant communications; others are more sceptical and warn of "the Net illusion". But it is certain that the empowerment effect is considerable. And it is double, since the new networks can also be used by authoritarian governments to relay regime propaganda

[7] And new interaction networks are springing up by the day, as for instance "google+".

and enforce repression. The new media "between revolution and repression[8]"!

The overall effect of the communication and information explosion of the last few years is in any event that governments wishing to establish or maintain control over their citizens and their access to information, and to stem instability and threats to their system, have to cope with a new dimension of the repression problem. This translates, in the practice of the last years, especially the last two years, into more repression and new repressive techniques.

The factual basis for observing this sad process exists. There are several organizations, including from academia, that operate observatories world-wide, identify and document cases, and report out in their comprehensive Internet pages. The most prominent ones – there are many others - , admirable in their thoroughness, professional rigor, and spread of research, are Freedom House, Reporters Without Borders, and the OpenNet Initiative[9]. They publish rankings of the governmental repressors on whom they collect information. Freedom House publishes annual reports on Freedom on the Net. On the basis of a detailed score table, the

[8] Reporters Without Borders, 2011 Report

[9] www.freedomhouse.org; www.rsf.org; http://opennetinitiative.net
. To be mentioned also are the Global Network Initiative,
http://globalnetworkinitiative.org
and Amnesty International.

organization allots an International Freedom Status designation. In its 2011 report, it ranks 11 countries as "not free", and 19 as only "partly free". Reporters Without Borders has a category of "Enemies of the Internet" where 10 countries are listed (they are essentially similar to the "not free" list of Freedom House), 16 other countries are placed "under surveillance". These lists comprise only the main offenders, on whom reliable information is available. Their geographical distribution is depicted in the two attached maps. Censorship mostly concentrates on political and national security content, but many countries go beyond. Intensity varies, but on the basis of the existing material one can assume that governments of more than 60 countries practice some form of censorship and that more than 25% of the current world population – Reporters without Borders speaks of one third! – live under censorship, - a staggering record.

Yet it is not so much the number of censoring countries – and thus of population – that has increased, but the intensity of control, and the number of new repressive techniques employed.

In our earlier work we concentrated our analysis on the censuring technique of content filtering by advanced routers, relying often upon foreign servers to install the corresponding software, and then block sites and practice surveillance; we were openly critical of what we saw as profit-oriented aiding and abetting in violation of ethical principles and international law. Filtering is still practiced at a massive scale by most repressive governments, – and augmented in period of unrest and Government nervousness –, but the shift away from the traditional www to new applications has also motivated a partial shift from content filtering and site blocking to new methods. At the same time, many developing countries are advancing in their own filter technologies and are taking the server structure into their own hands, thus depending less on foreign software technology imports and the readiness of foreign Internet service providers to obey their repressive orders. These new national infrastructures, often highly centralized, easily turn into Big Brother, Orwellian control mechanisms. However, the pressure on foreign service providers has also notably grown in some countries, thus heightening their ethical dilemmas.

Many repressor countries have responded to the growth in the number and nature of information stakeholders by a noticeable acceleration of reactions to the appearance of undesirable sites, and by institutionalizing their censoring agencies, – in some cases these are huge, and technically competent. These countries tend to move from intermittent interferences to a much more intensive, agile and intrusive system of control. More sites are being controlled and interfered with, and sanctions become more severe.

Generally speaking, it can be observed that repressor governments move from whole-sale blocking and shutting down of certain sites to individual persecution. Massive, clearly directed DDoS attacks, espionage, defacing of individual pages, phishing, password theft, falsification of information and sites supplement general filtering. These attacks are often performed, at State behest, by hired non-State hackers. The harassment and terror effect of these individualized attacks is clearly designed to muzzle dissident opinions.

One increasingly frequent technique is the temporary slow-down in band-width speed (total, or geographically limited), with the effect that big data packets, photos and videos can no longer be received or sent. This strategy is increasingly applied in periods of turmoil – or expected turmoil – and political tension, like recently in the Middle East. As has been observed, in countries like Iran, but also Egypt at the time of unrest, "connection speed has become the barometer of a country's political and social situation[10]". At times, this technique is accompanied by jamming or a shut-down of cell phone networks in relevant areas.

Blogs and the new social networks, as the perceived main agents of undesired political activity, are preferred targets of the new wave of cyber repression. Prominent bloggers are individually persecuted

[10] Reporters Without Borders, March 2011 Report, p.5

and castigated with shut-downs. Bloggers receive personal threats. The history of total, or just-in-time, blockings of Twitter, Facebook and the like is long; often these shut-downs are timed to coincide with periods of unrest. The technology and case history of these shut-downs will be dealt with in more detail in another presentation in this session. Repression of the New Media is particularly grave as, beyond filtering out information and limiting individual exchanges of opinion, it impedes the operation of a new universe of collective opinion-forming and mobilization.

There is often ruthless criminal persecution of cyber "offenders". Key repressor countries have a dedicated cyber police who intimidate and threaten, but also act. Arrests of bloggers and "netizens" in the key repressor countries continue unabated. Reporters without Borders keep track: as of March 2011 there were 119 perpetrators in jail, including 2011 Nobel peace prize winner Liu Xiaobo. In Iran, there have been the first condemnations to death. Many of the police actions are directed against users of the New Media, as they are perceived to be the principal virtual meeting place of adolescent political dissenters. In one of our earlier documents we unabashedly asked to what extent foreign software producers and service providers are – directly or indirectly – responsible for these "cyber criminals" to be denounced and condemned.

Another new feature of the cyber repression scene is that repressor governments do not content themselves with impeding undesirable information traffic and enact reprisals, but move to affirmative action. The new battle is about manipulation of information. Repressive governments increasingly and proactively use the new social networks for massive propaganda and distortion of facts to counter the Facebook and Twitter effect. Here again, the duplicity, the ambivalence of new technologies, in this case the social networks, shows clearly.

Our PMP has always thought that wailing and denouncing in the face of a common evil is not enough: we have always placed our analysis in an operational perspective, coupling it with precise recommendations, a time-proven Erice recipe. Many of the afore-named organizations that are admirable in their analysis and voice their revolt, fail to proceed beyond that passive stance. However, the worsening situation of cyber repression makes action more necessary than ever

I will thus briefly review the action plan which has been part of our earlier documents, and will try to indicate where our operational options can be reinforced, and what else we can do.

Action can and should be taken by civil society – the articulate lobby for a Free Internet - , by industry, by governments, and – most important – by the international community. Our earlier documents list the organizations that strive for freedom of expression in the Internet, denounce the wrongdoers, sensitize public opinion, and help the victims of cyber repression by providing evasion techniques to bypass censorship, anti-filter software and the like. This assistance is effective where the "traditional" filtering methods are used, but cannot cope with the new techniques repressive governments apply, - especially when there are shut-downs, reduction of bandwidth speed, large-scale manipulation of information, or individual attacks and reprisals. Yet, the efforts of the Internet lobby are praiseworthy, and there should be more mobilization, especially in many countries not yet involved, to join or do likewise. The OpenNet Initiative and the Global Network Initiative are among those deserving particularly strong support.

Governments can do a lot. The US Government is exemplary in its support for Internet freedom which includes the creation of the Global Internet Freedom Task Force and the provision of funds for assisting filter circumvention technologies. The European Union does not accept export of filter software technologies to repressor countries. Indeed there should be global export controls for this purpose.

The principal areas where more action should be deployed are the public arenas of the International Community: international fora and international organizations. Practically the entire world community has subscribed to the Universal Declaration of Human Rights and the two International Covenants, thus converting the principle of freedom of expression into international law of general validity. They all share a common responsibility. It is their duty collectively to respect, protect, promote and fulfil human rights, including the freedom of expression. We should therefore urge more strongly – and bring this to our governments - that the struggle against cyber repression be carried into international organizations that have a calling in this field. A call from the World Federation of Scientists to this effect could make a difference and produce impact..

In our earlier documents we have discussed the pros and cons of each one these relevant international bodies. We have also argued that an international complaint procedure of the "comply or explain"-type be introduced that, - as direct sanctions are not feasible - would increasingly put international pressure and opprobrium on repressive Governments. In the interest of brevity, I will only refer to these texts and will merely list the organizations we have considered:

- The World Summit on the Information Society. We brought the case to the 2003/2005 First Summit. It did not take up our proposals for pertinent resolutions, but in its Geneva Declaration of Principles has strongly affirmed extant international law on freedom of expression. Governments should build on that to introduce the topic into the agenda for the forthcoming 2015 Second Summit.
- The Internet Governance Forum
- UNESCO as, by its founding act, the unique international guardian of freedom of information, and, in addition, mandated by the WSIS (and the UNGA) to deal with the topics of "Access to Information and Knowledge", and the "Ethical Dimension of the Internet"
- The UN Human Rights Council as the special body dealing with violations of the International Covenant on Civil and Political Rights which cyber repression violates; it could establish the suggested complaint procedure, and/or include the topic of Internet Freedom and censorship in the statutory Universal Periodic Review Process.

- Finally, the UN Human Rights Committee which is entrusted with periodic country reviews. These should in the future include Internet Freedom.

A Postcript:

Wikileaks vs. Government Controls

When this presentation was commissioned, the problem of Wikileaks vs. Government Control also figured in the assignment. As I have not treated it in the body of the text, a brief supplementary note on it might be in order.

Discussing Wikileaks, and especially the recent massive release of confidential government papers, predominantly from the US Government, is not, properly speaking within the purview of this presentation: no repressive government has been at work, and developing countries and their legal systems are not involved. In fact, the leaks concern some of the freest countries in the world, where, in addition, legal procedures are available to enforce Freedom of Information (e.g. under the US Freedom of Information Act).

But the Wikileaks case does, in fact, pose the question of the inherent tension between public order and security on the one side, and totally unbridled openness on the other. From the viewpoint of the Erice community, the Wikileaks perpetrators have promoted freedom of information and expression, and have thus done something positive. Most of the information, in addition, does not apparently affect State security or, in most cases, betray essential State secrets; most of the effect has been no more than embarrassing and damaging to the prestige, if not the vanity of those who would have preferred to preserve confidentiality. As some of the material uncovers illegal practices by a government, - for example, corruption cases in Hungary or Tunisia - additional healthy effects may have occurred, and in some contexts opposition forces may have benefitted.

But this positive assessment has to be nuanced in two important ways. From an information security standpoint, there are probably massive elements of interference with the Internet and computer systems (illegal interception, data interference, system interference), punishable under the applicable national cybercrime legislation. If there was printed material – or any other material, like a CD Rom - involved, the perpetrators have committed theft. There may also be illegal acquisition if other protected interests have been affected (e.g. intellectual property rights). Furthermore, for some part of the material, State secrets may have been involved: this has been claimed by the Australian Government, and the Espionage Act may apply for the US if protected secrets have been disclosed within the country. A detailed analysis in the light of each national legal system would be necessary to determine whether penal laws apply. Government insiders with authorized access – like Pfc. Manning in the recent Wikileaks disclosure – may be subject to disciplinary or even penal sanction if classified information was revealed.

The other nuance is more of a philosophical nature. Society is made up of competing goods, this competition cannot be resolved in a once-for all way but requires the earnest search for acceptable equilibria. When State documents are involved the tension, referred to above, between security and individual liberty takes on a special twist. Statecraft, even beyond the formal qualification of State secrets, requires a margin of confidentiality to be effective; take international negotiations and their ever-changing tactical needs. Statecraft and total transparency are not compatible, and for statecraft not to be wrecked, some limits to transparency must be preserved. Call it maturity? Responsibility? Patriotism? In this perspective, Wikileaks cannot endure with its present absolute quest for total transparency. Already, it has done damage.

The consequences will possibly result in more damage. If Wikileaks does not mend its ways, Governments will become more restrictive in their information policy, clamp the stamp of "State Secret" on more, otherwise innocuous documents and restrict the freedom of information and opinion of which we, members of open democratic systems, are justly proud.