ODUMUNC 2010
Issue Brief for the
GA First Committee Disarmament and International Security (DISEC)
Selected readings on

Balancing International Security and Freedom of Information

PARTICIPANTS IN UNITED NATIONS FORUM ON INTERNET GOVERNANCE ADDRESS: KEY THEMES OF NET OPENNESS, SECURITY AT RIO DE JANEIRO EVENT

14 November 2007

United Nations

Press Release

PI/1814

Department of Public Information • News and Media Division • New York

RIO DE JANEIRO, 14 November -- Openness and security of the web were the main themes at today's session of the Internet Governance Forum, which is gathering in Rio de Janeiro more than 1,700 participants from Government, civil society, the private sector and the Internet community.

Ronaldo Lemos, Law Professor at Rio de Janeiro's Centre of Technology and Society, opened the morning session. Openness, he said, had legal, political and economic dimensions. One legal issue that had to be regulated locally was the liability of online service providers, but most countries had yet to address it. On the economic front, openness was related to the lack of interoperability of Internet systems, which generated costs that developing countries could not afford. But openness also lowered the barriers for new entrants in economic markets, thus fostering innovation.

David Gross, Coordinator for International Communications Policy at the United States State Department, said the Tunis Commitment adopted at the 2005 World Summit on the Information Society (WSIS) recognized the importance of encouraging the free flow of information, ideas and knowledge, which were essential for the information society and beneficial to development. Each country should determine how to implement that recognition, in a democratic fashion and reflecting the country's culture and norms, but with an eye towards that principle.

Masanobu Katoh, Corporate Vice-President at Fujitsu Ltd., said neither freedom of information nor regulations should prevail over each other. For many, “IP” did not mean “Internet Protocol” but “Intellectual Property”. Internet experts felt freedom of expression was paramount, and intellectual property experts felt the same about intellectual property rights. The two could coexist, as shown by legislation and guidelines adopted by the United States Congress, the European Parliament and Japan.

Self-regulation by the private sector should supplement Government action, he said. It could be more efficient and avoid some of the risks of the “surveillance society”. The dichotomy between Internet freedom and Internet regulation could be resolved by striking a balance among competing interests and by combining laws with guidelines established by the private sector.

Mark Kelly, an international human rights lawyer, stressed the public service value of the Internet. The web had become an integral part of people's lives, and people relied on it with the expectation that it would be affordable, secure, reliable and enduring.

But the public service value of the web was not being respected by all groups, he said. States had become accustomed to being held accountable for respecting Internet freedom as recognized in the WSIS outcome documents. But two years after WSIS not all parties were playing their part, especially the Internet Corporation for Assigned Names and Numbers (ICANN) and private companies, not all of which had incorporated a real human rights approach in their decision-making.

Alexandre Jobim, Chairman of the Legal Committee of the International Association of Broadcasters, said broadcasters were held strictly accountable, for instance through laws prohibiting child pornography and incitation to violence. But those same restrictions did not apply to the Internet, leading to an unfair imbalance between strong regulations for print and broadcast media and much looser regulations for Web-based media. Broadcasters fully supported Internet freedom, but saw the need to limit online criminal activities.

Nick Dearden, Campaign Manager for Amnesty International, said Internet filtering was spreading rapidly, activists were imprisoned for legitimate online activities and companies cooperated with Governments in censorship. “As Internet access continues to grow, this repression seems certain to increase as well.” That could threaten ultimately the nature of the Internet itself, turning it into “a tool of repression and limitation rather than liberation and openness”.

“For many Governments across the world, human rights are actually slipping down the agenda,” he said. Governments were concerned about credit card frauds, child pornography and cyberterrorism but seldom mentioned freedom of expression. Current Internet problems should be addressed, but always taking freedom of expression into account.

ICANN Chairman Peter Dengate, also an intellectual property lawyer, said freedom of expression was sacrosanct, but there was also the “freedom to enjoy the fruits of your labour and the freedom to enjoy the undisturbed use of your property”. The Internet made the copying of people's property “extraordinarily easy”. Images, music and texts could be taken and used instantly, without having the authority, leading to a potential conflict between the two freedoms.

Copyright law had developed on the notion of a fair use of other people's property, and had tried to balance the owner's exclusive right of use with the right by others to use, he said. Copyright did not protect ideas but the expression of the ideas, and there was no conflict between copyright and freedom of information. Once the issues were separated, there was no contradiction between protecting the idea and protecting the effort that someone had made in turning an idea into a useful product. In drawing the boundaries of intellectual property law, one should recognize that those boundaries shifted as the community shifted, and with the Internet came innovative solutions to the problems it posed.

Carlos Gregorio, an expert on privacy rights, said openness was the balance amongst the right to access, the right to freedom of expression and the right to privacy. Everybody wanted to keep the greatest openness possible, but openness could also make people vulnerable, and the main creator of such vulnerability was the State. In Latin America the State exposed people unnecessarily. Many of the websites of the judiciary had been made public in the name of transparency, but people with HIV/AIDS had suffered because of that openness. One Latin American country had almost all people living with HIV/AIDS online, with names and social security numbers, and most of them were children.

He said workers who had sued their former employer were made vulnerable because the verdict was available on-line, ensuring that they would never by hired again. A Mexican company checked every day the websites of the judiciary, and then sold the results to the personnel office of companies.

Teenagers took normal pictures, changed them into pornographic photos and posted them on the web for sexual harassment, he said. “The Internet is open, but it is not a space for irresponsibility. There should be rules, rules where you can have criminal and civil punishment.”

Freedom of expression was made vulnerable when the priorities of access to information were established by Google, Alta Vista, and other companies, he said. “Privacy, regrettably, is being lost. And it will be very difficult to keep it up.”

The afternoon session on Internet security was opened by Antonio Tavares, Representative of the Private Sector at Brazil's Internet Steering Committee, who said that 95 per cent of crimes committed on the Internet were already covered by existing legislation.

Ralf Bendrath, Research Fellow at Bremen University in Germany said security could be approached as security of computers at the end point of the net, security of companies, protection against fraud and cybercrime, but also as better security for the user, to which greater attention should be paid. Total security was impossible, yet politicians tended to ask for more and more security, and there was a need to decide where to draw the line and acknowledge that a satisfactory level of security had been reached. Rather than talking about network security, it was better to talk about network reliability, which was achieved with the web delivering daily huge information packages all over the world.

Huang Chengqing, Secretary-General of China's Internet Society, said one dimension of Internet security involved law enforcement and countering crime. All over the world, cyberattacks and Internet frauds had increased much faster than the Internet growth rate, and cooperation between business and civil society was essential. In the first quarter of 2006, 21 per cent of the world's spam had come from China, which had since adopted anti-spam legislation and administrative measures. Spam had gone down to 4.9 per cent.

Lamia Chaffai, Director of the Tunisian Internet Agency, and Christine Hoeler's of Brazil's Computer Emergency Response Team also called for cooperation among business, civil society and regulators in order to adopt policies, legislation and technical solutions and to standardize rules.

Marco Gercke, Professor of Criminal Law at Cologne University in Germany said law-enforcement agencies needed to cooperate across borders, which was not happening enough. There was only one international treaty against cybercrime, the Council of Europe's Cybercrime Convention, which was open to all countries and had been signed by 43. Most of the signatories were technically advanced countries, and the Convention had not involved developing countries enough. Yet in 2005 the number of Internet users in developing countries had surpassed that of users in developed countries. There was a need to standardize norms, involving especially developing countries. The Convention had created a committee for legal standardization among signatory countries.

Zahid Jamil, a lawyer from Pakistan, said his country had adopted cybersecurity laws following the killing of Wall Street Journal journalist Daniel Pearl. However, the laws had proved too draconian, and Pakistan had worked with the Council of Europe to adapt the Cybercrime Convention to its specific needs.

***Marching off to cyberwar*, The Economist**. London: 6 Dec 2008, vol. 389, no. 8609

AS RUSSIAN tanks rolled into Georgia in August, another force was also mobilising--not in the physical world, but online. Russian nationalists (or indeed anyone else) who wished to take part in the attack on Georgia could do so from anywhere with an internet connection, simply by visiting one of several pro-Russia websites and downloading the software and instructions needed to perform a "distributed denial of service" (DDoS) attack. This involves sending a flood of bogus requests to an internet server, so that it is overwhelmed by the demand and becomes unusable.

One website, called StopGeorgia, provided a utility called DoSHTTP, plus a handy list of target websites, including those of Georgian government agencies and the British and American embassies in the capital, Tbilisi. Launching an attack was as simple as entering the address and clicking a button labelled "Start Flood". The StopGeorgia website helpfully indicated which target sites were still active and which had collapsed under the weight of bogus requests. Other websites explained how to write simple programs to send a flood of requests, or offered specially formatted webpages that could be set to reload themselves continuously, deluging particular Georgian websites with traffic.

The actual damage done was minimal: some e-mail was disrupted and some target sites were rendered unavailable to the public. The cyberattacks on Estonia in 2007, also launched from Russia, were more effective because Estonia's government relies far more heavily on the internet (its parliament declared internet access a human right in 2000). They briefly upset the operations of some government organisations, including telephone access to the emergency services.

There is no conclusive evidence that either set of attacks was executed or sanctioned by the Russian government--though there is no evidence that it tried to stop them, either. Ethan Zuckerman, an internet expert at Harvard, has described the plethora of competing theories as "the fog of cyberwar". And in the Georgian case volunteer cyberwarriors--dubbed "a citizen DDoS army" by Artem Dinaburg of Damballa, a cybersecurity start-up--were also involved. Does any of this really count as an act of war? The Estonian and Georgian cyberattacks have put to the test a host of theories about cyberwarfare: how to define it; whether to engage in it; and how to defend against it. A definition of war

The discussion of cyberattacks and cyberwarfare is complicated by widespread disagreement over how to define these terms. Many cyberattacks are really examples of vandalism or hooliganism, observes Bruce Schneier, a security guru who works for BT, a British telecoms operator. A cyberattack on a power station or an emergency-services call centre could be an act of war or of terrorism, depending on who carries it out and what their motives are.

For a cyberattack to qualify as "cyberwar", some observers argue, it must take place alongside actual military operations. Trying to disrupt enemy communications during conflict is, after all, a practice that goes back to the earliest telecommunications technology, the telegraph. In 1862, for example, during the American Civil War, a landing party from Thomas Freeborn, a Union navy steamer, went ashore to cut the telegraph lines between Fredericksburg and Richmond. The Russian navy pioneered the use of radio jamming in the Russo-Japanese war of 1905. On this view, cyberattacks on infrastructure are the next logical step. The attacks on

Georgia might qualify as cyberwarfare by this definition, but those on Estonia would not, since there was no accompanying military offensive in the real world. As Mr Schneier puts it: "For it to be cyberwar, it must first be war."

Not everyone agrees. For years there has been talk of a "digital Pearl Harbour"--an unexpected attack on a nation's infrastructure via the internet, in which power stations are shut down, air-traffic control is sabotaged and telecoms networks are disabled. There have even been suggestions that future wars could be waged in cyberspace, displacing conventional military operations altogether. Why bomb your enemy's power-stations or stockmarkets if you can disable them with software? So far there have been no successful attacks of this type, but that does not stop people worrying about them--or speculating about how to launch them.

The strongest definition of cyberwar requires that cyberattacks cause widespread harm, rather than mere inconvenience. The Georgian attacks did not cause physical harm, unlike the military operations going on at the same time.

Such definitions matter because cybervandalism or cyberhooliganism are forms of cybercrime, which (in theory at least) is dealt with by various national and international law-enforcement agencies according to existing legal conventions, such as the Council of Europe Convention on Cybercrime. A private individual in Russia who defaces an Estonian website ought to be treated in a similar fashion to his neighbour who travels to Tallinn, breaks a shop window and goes into hiding in Russia--though identifying a cyberattacker is far from easy and after the attacks in 2007 the Russian authorities refused to co-operate with Estonian investigators.

Such was the intensity of the attacks on Estonian websites, however, that the country's defence minister, Jaak Aaviksoo, warned that the action "cannot be treated as hooliganism, but has to be treated as an attack against the state". But treating the attacks as acts of war would mean applying a different set of rules, presenting a new challenge to policymakers.

All sorts of "translation problems" arise when trying to apply existing international rules relating to terrorism and warfare to online attacks, says Duncan Hollis, a professor of law at Temple University in Pennsylvania. The United Nations Charter prohibits the use of force except when authorised by the Security Council, for example, but does not spell out what counts as "the use of force" in cyberspace. Do DDoS attacks count? Perhaps not if aimed at a newspaper website, but what about an air-traffic control system?

Agreement on a definition is needed, says Mr Hollis, because under international law a country that considers itself the victim of an act of war has the right to self-defence--with conventional military (not merely electronic) means. And members of an alliance with mutual-defence obligations, such as NATO, may be duty-bound to respond to an attack on any of their members. So the cyberattack on Estonia, a NATO member, could in theory have prompted a military response. To grapple with questions like these, and to bring together a group of experts in "cyberdefence", NATO has set up a research centre in Tallinn, which is already open but will be formally inaugurated in 2009.

Mr Hollis points out that the debate about how best to classify cyberattacks has much in common with the debate about terrorism. Should terrorism be treated as a crime, as an act of war, as both at once, or as something entirely different that requires new laws? He favours this last approach for cyberattacks because it avoids the translation problems that arise when applying existing rules to such attacks, and because those rules are themselves somewhat outdated, given that attacks (in the real world and online) may come from non-state actors such as terrorist groups. Mr Hollis proposes a new "international law for information operations" to alleviate the uncertainty. He concedes that there is unlikely to be international consensus in this area soon, but argues that it would be a big step in the right direction if a group of states such as NATO, or the OECD club of industrialised nations, agreed to be bound by a clear set of rules.

What effect such co-operation would have on containing anonymous and unofficial cyberwarriors is hard to say; the fight against real-world terrorism does not offer much hope. And it is attacks from such groups that some researchers are most worried about. John Robb, a military futurist, calls the spontaneous, bottom-up mobilisation of volunteer cyberattackers in the Georgian conflict an example of "open-source cyberwarfare".

This approach has several advantages over centralised, state-directed cyberattacks, he says. Leaving the attacks to informal cybergangs (the extent of the Russian state's involvement remains unclear), rather than trying to organise a formal cyberarmy, is cheaper, for one thing. The most talented attackers, with the best tools, might not want to work for the state directly. Best of all, from the state's point of view, is that it can deny responsibility for the attacks. It is the online equivalent of the use, by some governments, of gangs and militias to carry out attacks on political opponents or maintain control in particular regions. Send in the botnet

There is no consensus among conventional military types about how to deal with such cyberattackers. Writing in Armed Forces Journal in May, Colonel Charles Williamson, of the intelligence and surveillance division of America's air force, proposed that the United States should establish its own "botnet"--a network of machines "that can direct such massive amounts of traffic to target computers that they can no longer communicate and become no more useful to our adversaries than hunks of metal and plastic." America, he wrote, "needs the ability to carpet-bomb in cyberspace to create the deterrent we lack." The botnet could be built out of obsolete computers that would otherwise be discarded, he suggested. But he conceded that there would be legal and political difficulties associated with its use.

Mr Robb is sceptical of the ability of formal military organisations to wage cyberwarfare. "A few top people with the right tools can do the work of thousands of less capable people, so it's better not to waste the money on 40,000 uniformed personnel dedicated to a bureaucratic and lethargic cyber command," he says. And after an attack from an informal, self-organised group, there is no clear target to strike in any case. It may make more sense for existing military bodies to concentrate on defence, by identifying the most vulnerable parts and working out how to protect them. "Anything they can do to us, we should be able to counter faster--that's the appropriate deterrence paradigm for this cyberage," says Thomas Barnett, a military strategist at Enterra Solutions, a technology firm. "We should concentrate on making ourselves resilient."

One way for governments to do this, says Richard Bejtlich, a former digital-security officer with the United States Air Force who now works at GE, an American conglomerate, might be to make greater use of open-source software, the underlying source code of which is available to anyone to inspect and improve. To those outside the field of computer security, and particularly to government types, the idea that such software can be more secure than code that is kept under lock and key can be difficult to accept. But from web-browsers to operating systems to encryption algorithms, the more people can scrutinise a piece of code, the more likely it is that its weak spots will be found and fixed. It may be that open-source defence is the best preparation for open-source attack. "

The United Nations Charter does not spell out what counts as "the use of force" in cyberspace."

Music piracy: Singing a different tune, 12 November 2009, **The Economist**
http://www.economist.com/businessfinance/displaystory.cfm?story_id=14845087

The battle against online music piracy is turning. A return to growth will take a good deal longer

ODUMUNC 2010
Issue Brief for the
GA First Committee Disarmament and International Security (DISEC)
Selected readings on

Balancing International Security and Freedom of Information

“ROCK and roll is dead,” sang Lenny Kravitz. It is certainly poorly. Music was the first media business to be seriously affected by piracy and has suffered most severely. Yet the prognosis is improving. While it is by no means over, the struggle against music piracy is going better than at any point since the appearance of Napster, a file-sharing service, ten years ago.

It has been a brutal decade. In many countries music sales to consumers have fallen by more than a third. Even Apple’s popular digital iTunes store is little more than a niche service: fully 95% of downloads are illegal, according to the International Federation of the Phonographic Industry (IFPI), a trade group. Established bands have been able to raise ticket prices in response. But by reducing the money available to sign and tout new artists, file-sharing has made it harder for bands to become established. Paul McGuinness, who manages the band U2, says the whole “starmaking apparatus” is damaged.

The music business is now doing two things right. First, it has built a better stick. Most countries have virtually abandoned the practice of suing people for downloading copyrighted files. The favoured approach these days is known as “graduated response” or “three strikes and you’re out”. People who are suspected of trading media illegally are sent warnings. If they fail to stop, their internet-service provider (ISP) may slow their connection. If that fails to deter, they may be temporarily cut off.

Graduated-response laws appeared this spring in Taiwan and South Korea—an advanced market where digital music has overtaken sales of CDs and DVDs. In October, following many political and legal hitches, they were enacted in France. The British government is expected to announce similar measures on November 18th. Almost everywhere in the developed world, such laws are being debated. Even where they are not (America, for example), ISPs are working quietly with the record industry to similar ends.

The trouble with the old practice of suing people for swapping music is that it is slow, expensive and limited. In most countries, being prosecuted for file-sharing is a little like being struck by lightning. The exception is Germany, where a cheap, efficient legal system has made it possible to launch some 100,000 prosecutions. In the past two years the proportion of German internet users who share files illegally has dropped significantly. It now stands at 6%, according to Jupiter Research—less than in any other big European country. Graduated response ought to make it possible to reach many more people, reckons Steven Marks, general counsel for the Recording Industry Association of America.

The second change is that the industry is offering tastier carrots. These days the music associations talk less about lawsuits and more about cultivating alternatives to piracy. The past year has seen rapid growth of digital music services that accept the post-Napster consensus that music should be free, or at least appear to be free. The companies involved range from Google, which now facilitates music streaming from its search page in America, to Nokia, which bundles access to a music-download service with some of its mobile phones. “The next big thing is a dozen different things,” says Thomas Hesse of Sony Music Entertainment.

The hottest product is Spotify, which has been downloaded to 6m computers in Europe. Spotify streams tracks free, interrupted by minimal advertising. Customers can pay a monthly fee to get rid of the advertisements or to install the application on iPhones and other mobile devices. Although streaming a song is not the same as owning it, Spotify has proved a compelling alternative to illegal file-sharing.

Ahoy there, me hearties

The effect is clearest in Sweden. That country incubated Spotify and The Pirate Bay, a popular website that allowed people to find pirated files easily. In April four people associated with the website were found guilty of copyright infringement. At about the same time Sweden enacted a law forcing ISPs to reveal more information about their subscribers. In the past, such legal actions have led music fans to find new ways of sharing files. Not so this time. In June a poll carried out by GfK, a market-research firm, found that 60% of Swedish file-sharers had cut back or stopped altogether. Of that group half had resorted to advertising-supported streaming.

Potentially more important are the efforts of ISPs, such as Virgin and BSkyB in Britain, to sell subscriptions to broadband and music together. Internet bills are often paid by parents who may wish to remove the temptation for their children to use peer-to-peer services. Such deals should also prod ISPs into a more active role in discouraging file-sharing. They are likely to become more involved if video piracy continues to grow, in any case. Many broadband suppliers are also in the pay-television business. If Comcast ends up buying NBC Universal a broadband supplier will own a film studio.

The pioneer of this model is Denmark’s incumbent telecoms firm, TDC, which offers more than 5m songs. Some 120m tracks have been downloaded so far, which works out at 22 per Dane. The tracks self-destruct shortly after a consumer lets his subscription lapse. Yet they seem to be a good enough substitute. Earlier this year more than two-fifths of TDC Play users told Megafon, a pollster, that they were downloading fewer illegal files. TDC likes the arrangement, too, because it makes customers more loyal.

The recorded-music business is not about to lurch into growth. A big proportion of revenues—more than half just about everywhere—still comes from CD albums, which are gradually falling out of favour. Start-ups like Spotify need to turn more freeloaders into paying subscribers if they are to survive and start providing a serious income stream to record companies and artists. And there are still plenty of ways of sneakily copying music.

John Kennedy, head of the IFPI, points out that piracy was rife even before file-sharing. The goal is not to eradicate it—that is impossible—but to tilt the playing field towards legitimate services. That finally seems to be happening.