Cyber Security, Cyber Surveillance and Online Human Rights

Anja Kovacs – Internet Democracy Project
Dixie Hawtin – Global Partners and Associates[1]

If activists are to win the fight to keep the Internet free and open, it is becoming increasingly clear that they must familiarise themselves intimately with the areas of cyber security and cyber surveillance. International state-sponsored cyber espionage has given birth to the twin narratives of cyber war and a cyber arms race; narratives which are being used in some parts of the world to encourage citizens to trade in civil liberties for a greater sense of security. In the US, for instance, cyber espionage by Chinese hackers is a key argument used to support the controversial Cyber Intelligence Sharing and Protection Act (CISPA) which would enable the authorities to access vast amounts of user data without a warrant.

Elsewhere, internal threats to national security posed by the use of new technologies have long been used to justify extensive surveillance measures. For example, in India, it is not possible to access mobile phones or Internet connections, including in cyber cafes, without official identification, and both ISPs and cyber cafes are required to maintain detailed logs of users' browsing history. The narratives of doom that invariably accompany such measures draw further strength from the very real growth of cyber crime – there are now said to be more than 150,000 viruses and other types of malicious code in circulation, with a million people becoming victims of cyber crime every day[2]. So while cyber security is not a new concern, in the last few years it has come to increasingly dominate and drive the Internet policy and governance agenda, as well as international policy discourse more broadly.

Genuine threats do indeed exist. Illegal access to computers and data, as well as data interference, have become more common and complex problems that affect large numbers of people. Issues like fraud are taking

[1] The authors would like to thank Grace Githaiga and Marcin de Kaminski for their inputs into this paper.
[2] 'Cyber crime'. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm. Last accessed 7 May 2013

on new forms on the Internet. And as more of our critical infrastructure becomes reliant on the Internet, security infringements can have significant repercussions, including for human rights when, for instance, an attack prevents people from accessing public services or exercising their right to expression. Where governments identify security threats, these should, therefore, not be made light of a priori. It is an integral duty of any state to ensure the security of the people within its boundaries, and this duty does extend to the cyber domain.

However, cyber security strategies must be designed and implemented in a way which is consistent with international human rights law – too often this is not the case, as seen in the surveillance regimes discussed above. In other cases, States have been found to be behind threats such as cyber attacks aimed at human rights defenders or the political opposition. It is therefore important that the broader human rights community starts engaging with these discourses more closely, to unpack the proclaimed threats as well as their supposed solutions and to ensure that human rights standards are upheld in the cyber security arena too. In what follows, we hope to contribute to such efforts.

Concerns about Current Cyber Security Debates and Practices

At present, the term "cyber security" lacks definition as it is used to cover a vast range of concerns: in different contexts and by different actors the term is used to refer to security of national infrastructure; security of Internet infrastructure; security of applications and services; security of users (ranging from businesses to individual users); to the stability of the State and of political structures. This inexact terminology points to one of the primary concerns about this growing discourse: the terminology covers an agenda which is inexact, mixes legitimate and illegitimate concerns and conflates different types and levels of risk. This prevents genuine objective scrutiny, and inevitably leads to responses which are wide-ranging and can easily be misused or abused.

Obscuring the role of the state in creating insecurity

Among the important issues that are obfuscated by the current lack of precision in cyber security debates is the fact that rivalries between States are among the chief security threats, with the narratives of cyber war and a cyber arms race rapidly gaining ground at the inter-state level. In particular, a number of countries are reportedly investing heavily in developing offensive capabilities. In recent weeks there have been reports that the Pentagon is fast-tracking cyber weapon development and acquisition through a process separate from that used for conventional

weapons[3]. China too, in considered a major investor in cyberwarfare capacity. And in the UK, official statistics show that 59% of the planned spend of the country's Cyber Security Strategy "is meant to go to the intelligence agencies". According to a senior officer from Cheltenham, "GCHQ's offensive capability gives the UK an edge... a large proportion of that money has [therefore] gone into those capabilities".[4]

Examples of state-sponsored attacks do exist for states to point to in their arguments about the need for such investment: Russia allegedly launched DDOS attacks that paralysed Estonia's banking system and civil services during a 2007 diplomatic dispute, and most famously, the United States and Israel allegedly used a computer worm, Stuxnet, to sabotage uranium enrichment facilities in Iran. In both the examples mentioned above, the damage was temporary and the threat could quickly be neutralised, in part because of the amazing resilience of the Internet architecture. Interestingly, however, the techniques used in such instances are remarkably similar to those deployed by cyber criminals, indicating how governments are exploiting for their own ends the very same security breaches that they claim to fight[5]. The language of cyber war and a cyber arms race has made expanding budgets for the military and intelligence possible at times of general austerity for many countries, contrary to public perception this is not always for reasons of defence.

Discourses of cyber war and a cyber arms race have also built a market with lucrative opportunities for the many private businesses that seek to provide the technologies to deal with such purported threats. Indeed, narratives of cyber security prop up not only government power but big business as well, and the influence of the security industry on these debates should not be underestimated. The cyber security sector is estimated to be worth tens of billions of US dollars every year[6], and they are investing huge amounts of funds in lobbying politicians. A report by the Center for Responsive Politics found that in the US the number of lobbying reports which mentioned the term "cyber security" more than doubled from 2011 to 2012[7]. Industry actors are also behind much of the information driving the agenda; this is extremely problematic given their

---

[3] Howarth, C. (2013) Pentagon's Move to Fast-Track Cyber Weapons Will Upset China and Russia. Available at: http://www.policymic.com/articles/6730/pentagon-s-move-to-fast-track-cyber-weapons-will-upset-china-and-russia, Last accessed 14 May 2013

4 Urban, M. (2013). Is UK Doing Enough to Protect Itself from Cyber Attack? BBC News, 30 April 2013, http://www.bbc.co.uk/news/uk-22338204 Last accessed 7 May 2013.

5 Deibert, R. (2012). The Growing Dark Side of Cyber Space (... And What To Do about It). Penn State Journal of Law and International Affairs, 1(2). Available at: http://elibrary.law.psu.edu/jlia/vol1/iss2/3

6 Ibid

7 Pepitone, J. (2013) Cybersecurity lobbying doubled in 2012. Available at: http://money.cnn.com/2013/04/08/technology/security/cybersecurity-lobbying/index.html Last accessed 14 May 2013

vested interests. And the relationship between these businesses and governments is often secretive. The sale to authoritarian regimes of technologies that allow for extensive surveillance of citizens by companies based in the democratic world has long been criticised. More recently, a study found that 25 countries were using the surveillance software FinSpy against their citizens, including in democratic states. Neither the company, Gamma International, nor the governments involved disclosed the relationship[8].

Despite the prevalence of the language of cyber war, it is important to remember, however, that the cyber domain is very different from the offline domains (earth, air, sea, space) that the terminology of war comes from, and loaded terms such as "war" and an "arms race" are frequently inappropriate to describe what is going on. It is far more difficult to localise damage or attribute responsibility online than offline. Furthermore, what is often reported in the media as examples of "cyber wars" do not entail violence and should more appropriately be referred to as instances of "cyber espionage". Acts of espionage are usually governed by different legislation than acts of warfare.

In fact, the only cyber attack so far that has caused (or is believed to have caused) physical damage offline, and that therefore is almost unanimously agreed to be an act of war fare, is Stuxnet, pointing to the duplicitous role that the USA is playing in the cyber security arena. Where governments actively foment reasons for their citizens to fear for their safety unless they accept extensive surveillance measures and offensive capabilities on the part of the State, this is irresponsible governance.

Confusing the debate by conflating different challenges

More broadly speaking, there are two different types of threats that are conflated all too often in the cyber security debate:

1) *Threats where technology is integral to the risk* - this category refers to attacks, damage or access without authorisation to data, programs, computers or networks. It includes DDoS attacks, acts of cyber espionage and attacks that aim to sabotage critical infrastructure.

2) *Threats conducted over the Internet where it is not fundamental to that risk* – this category includes the distribution of spam, the publication of child pornography or the use of the Internet to plan a terrorist attack. In

[8] Perlroth, N. (2013) Researchers Find 25 Countries Using Surveillance Software. Available at: http://bits.blogs.nytimes.com/2013/03/13/researchers-find-25-countries-using-surveillance-software/ Last accessed 14 May 2013

these cases the issues are not illegitimate access or damage, but consent to the communication (for spam) and the nature of the content of the communication (for child pornography and crimes planned over the Internet). While technology may change the nature or reach of these crimes, it is not integral to their definition as such.

By collapsing the two categories – for example, by clubbing attacks on critical infrastructure together with spam, which could be regarded more appropriately as an annoyance rather than a threat – the very different nature of the challenges that they entail is obscured. This makes it easy to uncritically supplant the narratives of impending crisis that so often surround the former to the latter.

Another reason for not conflating cyber crimes in the narrow sense and crimes that merely use the Internet is that it conceals the fact that there are much clearer defined international standards regarding appropriate responses to the latter than the former. There remains a paucity of legal analysis using human rights standards of initiatives taken to protect computer systems and networks, including where these form part of the national infrastructure. This is in part because such an analysis would require greater technical knowledge; because the information about these initiatives is often not public; because the impact on human rights standards is therefore often less apparent; and because, until recently such initiatives were more likely to be private efforts and thus were less likely to have far reaching consequences while also being less visible. With countries across the world now adopting cyber security strategies, it is increasingly important that these are analysed using a human rights law framework.

In the case of content-related crimes, however, much work has in fact been done over the past few years – and especially since the publication of the report on the Internet and freedom of expression by UN Special Rapporteur on Freedom of Opinion and Expression Frank La Rue in June 2011 – to shed light on and develop appropriate responses to content that may seem to fall within the reasonable restrictions on freedom of expression accepted under international law.

However, governments frequently ignore such guidelines. As the Special Rapporteur pointed out in his report, all too often, content restrictions, while potentially legitimate in certain circumstances, are implemented "without any legal basis, or on the basis of broad and ambiguous laws, without justifying the purpose of such actions; and/or in a manner that is clearly unnecessary and/or disproportionate to achieving the intended aim".[9] This may well be, at least in part, because the sense of crisis and

9 La Rue, Frank (2011). Report of the Special Rapporteur on the Promotion and Protection of

complexity that surrounds the fields of cyber attacks and cyber warfare is being transferred on to the field of cyber security as a whole.

Adopting cyber security strategies that violate human rights.

The use of loaded, imprecise language has, indeed, had far-reaching consequences, as many governments are using vague internal and external threats as arguments to justify ever greater investments in cyber arms and mass surveillance schemes, and ever greater governmental control of the Internet and their citizens. The sense of alarm embedded in cyber security narratives has clouded the need to objectively and evidentially substantiate the likelihood and nature of the dangers at hand. It has also given rise to the impression that all responses are appropriate and legitimate. For example, as we pointed out earlier, in many countries, both democratic and non-democratic, the threats posed to national security have long been used to justify extensive surveillance mechanisms, with more and more citizen data collected and easily accessed by state authorities. Other ominous "security" measures include developing so-called "Internet kill switches" (the notion of shutting down the Internet in order to protect it), restricting the use of encryption, implementing filtering and blocking mechanisms and introducing real name policies. Such measures often pose threats to civil liberties, yet they tend to lack judicial oversight as well as public data on which to judge their effectiveness (often because of claims that disclosure would impact on security efforts). While it is not at all clear that they improve security, they frequently risk erasing the benefits the Internet brings.

"The same rights that people have offline must also be protected online" - this simple statement, adopted by a UN Human Rights Council Resolution on July 2 2012, confirmed what seemed obvious to human rights activists for many years[10]. It is extremely important, however, as it demonstrates government acceptance that there are clear international legal limits on the actions that they can legally take in the cyber-domain. Laws and practices which interfere with human rights online are only legitimate to the extent to which they fall within the narrow constraints allowed under international human rights law. It is therefore necessary to revisit the cyber security agenda in light of human rights standards and values.

---

the Right to Freedom of Opinion and Expression, Frank La Rue (A/HRC/17/27). New York, United Nations General Assembly, 16 May 2011, para 26. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf Last accessed 7 May 2013.

[10] UN Human Rights Council (2012). The Promotion, Protection and Enjoyment of Human Rights on the Internet (A/HRC/20/L.13). New York, United Nations General Assembly, 29 June 2012.

A Human Rights Approach to Cyber Security

From a negative to positive conception of cyber security

What, then, does a human rights approach to cyber security entail? First of all, such an approach puts the interests of citizens back at the centre of any cyber security policy. States tend to view security in the negative sense, as the mere absence of harm. The sole aim of any security policy then is to keep this harm at bay. Using this negative conception of security has led to policies and practices which disempower the people they seek to serve. What is more, those in power – in current discourses generally identified as governments or businesses – invariably benefit disproportionately in the process.

Debates around food and human security have amply illustrated, however, that security need not necessarily refer simply to the absence of harm. In a substantive sense, security is a positive concept: one that refers to a person's ability to gain access to a crucial resource and to use that resource according to their needs and preferences. A human rights approach to cyber security similarly foregrounds a positive understanding of security that focuses on people's capacity to act.

Where the Internet is concerned, security from a human rights perspective does not simply entail keeping people safe. Cyber security policies should not merely play a defensive role, but a facilitating role, by effectively putting the empowerment and well-being of people at their centre. What we are aiming for is for people to be able to be *fearless*, as long as they are respecting other people's human rights.

Ensuring "solutions" do not become threats

Defined in this way, a human rights approach to cyber security reminds us that in order to assess the effectiveness of a cyber security measure, it is essential to take into consideration not only the potential impact of the various threats to cyber security, but also the proposed solutions. If a measure taken in the name of protecting people from harm undermines their human rights in such a way and to such an extent that their ability to gain access to and use the Internet has been considerably impeded, it cannot be considered a reasonable security measure.

Such an approach immediately makes clear why cyber surveillance has become such a contested topic around the world. Though cyber security and surveillance are often mentioned by governments as two sides of the same coin, as if one somehow necessarily requires the other, the relationship between the two is actually a deeply uneasy one. Surveillance frequently requires or implies an increase in vulnerability, for example

when governments demand access to encryption or prescribe maximum levels of encryption. In the name of security, people are encouraged to give up the very tools – as well as agency – that allow them to protect themselves and to shape the Internet environment that they have defined for themselves as desirable. In most cases this is without it being clear precisely which threats are being addressed; how effective the responses are in doing so; and what the cost-benefit analysis from the perspective of Internet users is. Surveillance measures that are currently in place in countries from India to the UK fundamentally undermine the fearlessness of their populations when they come online. In fact, in the case of South Korea's real name policy, the policy was in fact found to make people more insecure, as the collected data was exposed through several high profile hacking attacks[11].

Many people do accept that government agencies might need to engage in cyber surveillance of specific individuals for specific reasons. However, surveillance needs to be both necessary and proportionate to the threat. These conditions are frequently unfulfilled. Rather than supporting each other, cyber security and surveillance are frequently at odds. If we are to develop cyber security policies that fundamentally support human rights, it is essential that this be recognised and accounted for.

Applying a Human Rights Approach to Cyber Security

International legal standards

Applying human rights law to cyber security debates, policies and practices will rely on all actors familiarising themselves with human rights standards and promoting them consistently. In recent years there have been a number of attempts to define exactly how international human rights standards apply to the internet environment. The reports of the UN Special Rapporteur provide a good understanding of how freedom of expression applies. The "International Principles on Communications Surveillance and Human Rights" (summarised in Box 1), describes the main principles of a human rights approach to cyber security as delineated by a group of civil society organisations, industry and international experts. Article 19's Johannesburg Principles on National Security provides principles for applying the legitimate aim of "national security".

11 http://www.freedomhouse.org/report/freedom-net/2012/south-korea

Box 1. International Principles on the Application of Human Rights to Communications Surveillance

In light of the proliferation of state surveillance of communications which does not adhere to international human rights law, a group of civil society groups, industry and international experts conducted a consultation about how existing human rights law applies to communications surveillance technologies and techniques. The result is the "International Principles on the Application of Human Rights to Communications Surveillance" released on 10 May 2013. Below is a summarised version of the principles (from http://www.necessaryandproportionate.net/):

- **Legality:** Any limitation to the right to privacy must be prescribed by law.
- **Legitimate Aim**: Laws should only permit surveillance to achieve a legitimate aim that constitutes an important legal interest that is necessary in a democratic society.
- **Necessity**: Laws must limit surveillance to that which is strictly and demonstrably necessary to achieve a legitimate aim.
- **Adequacy**: Any instance of communications surveillance authorised by law must be appropriate to fulfil the specific legitimate aim identified.
- **Proportionality**: decisions about surveillance must weigh the benefit sought to be achieved against the harm that would be caused to the individual's rights, and should consider the sensitivity of the information and the severity of the privacy infringement.
- **Competent Judicial Authority:** Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent.
- **Due process**: Lawful procedures that govern any interference with human rights must be properly enumerated in law, consistently practiced, and available to the general public.
- **User notification**: Individuals should be notified of a decision authorising communications surveillance with enough time and information to appeal the decision.
- **Transparency:** States should be transparent about the use and scope of communications surveillance techniques and powers.
- **Public oversight**: States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance.
- **Integrity of communications and systems**: States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for surveillance purposes.
- **Safeguards for international cooperation**: Where, under international agreements, the laws of more than one state could apply to communications surveillance, the standard with the higher level of protection for individuals should be applied.
- **Safeguards against illegitimate access**: States should enact legislation criminalising illegal communications surveillance by public or private actors.

Privacy and Freedom of Expression

Although other human rights (such as the right to peaceful assembly and association, the right to an effective remedy and the presumption of innocence) are also relevant, two human rights in particular will form the building blocks of rights-respecting approaches to cybersecurity. One is the right to privacy, or the right to keep one's data and communication away from the preying eyes of government, businesses or other citizens. The right to privacy is a necessary component in the development of a citizen-centric security policy. However it is not sufficient, as it does not exhaust the requirements for being secure online in the manner we defined above. For example, the right to privacy does not provide sufficient safeguards against content controls instituted by governments in the name of security policies at the locations where Internet cables enter a country. Privacy can be interfered with when a person is denied the confidentiality of their communications or control over information about them. In the assessment of cyber security policies equal stature should be given to the substantive enjoyment by all citizens of the right to freedom of expression. The other central right, freedom of expression, is interfered with when an action prevents someone from seeking, receiving or imparting any expression other than that which can be legitimately limited, and actions which "chills", i.e. discourages or inhibits, that expression.

Both of these rights can, by law, be restricted under certain circumstances. However, interferences with freedom of expression will only be legitimate if they follow the tripartite cumulative test being provided by law which is clear and accessible to everyone, for one of the purposes outlined in article 19 (2) ICCPR, necessary and the least restrictive means available to achieve that aim. Similarly, interferences with the right to privacy require that "there must be a law that clearly outlines the conditions whereby individuals' right to privacy can be restricted under exceptional circumstances, and measures encroaching upon this right must be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others, for example to secure evidence to prevent the commission of a crime, and must respect the principle of proportionality"[12]. These terms and tests have been developed and elaborated on through case law and soft law standards. Any security measure that does not adhere to these strict criteria, while possibly increasing the security of the network, undermines the substantive security of the people. It undermines fearlessness.

---

12 La Rue, Frank (2011), Report, para 59.

Contested issues

Whither anonymity?

Anonymous communication has played a crucial role throughout history in furthering contentious debates and revealing corruption and scandal in high places. In the Internet age, however, the ability to communicate anonymously is increasingly under threat. In a growing number of countries, the use of mobile phones, Internet connections and even cyber cafes is possible only after users have registered and provided extensive documentation. In some countries, real-name identification systems for the use of services once a user is online have also been suggested or implemented. Increasingly, intelligence agencies seem to effectively be tracking the activities of a wide range of users online – either of their own citizens or of citizens of other countries – without sufficient safeguards in place to protect users' right to privacy or the presumption of innocence.

In such circumstances, the ability to communicate anonymously is effectively destroyed, as is the presumption of innocence. As South Korea's Constitutional Court commented when assessing the constitutionality of the country's Internet Identity Verification Rule, systems that make it mandatory for users to provide identification data treat “all people as potential criminals”. The Court further observed that "Anonymous speech in the Internet, rapidly spreading and reciprocal, allows people to overcome the economic or political hierarchy off-line and therefore to form public opinions free from class, social status, age, and gender distinctions, which make governance more reflective of the opinions of people from diverse classes and thereby further promotes democracy. Therefore, anonymous speech in the Internet, though fraught with harmful side-effects, should be strongly protected in view of its constitutional values.”[13] Yet surveillance measures in many countries continue to undermine anonymity online.

Public-Private information sharing?

Such problems are compounded by the fact that many cyber security strategies create mechanisms to promote greater information sharing between private companies and government officials to allow improved responses to cyber security threats. To an extent this is an inevitable approach in a multi-stakeholder field where both actors hold parts of the information that is needed to successfully detect and counter threats. However, where close private-public relationships, including information-sharing, develop without adequate safeguards, this can easily

13 Quoted in Park, K.S. (2012). Korean Internet Identity Verification Rule Struck Down Unconstitutional; 12 Highlights of the Judgement. http://blog.naver.com/kyungsinpark/110145810944 Last accessed 7 May 2013.

lead to human rights violations. For example, in a recent long-running case in the US, it has been revealed that AT&T, a US telecommunications giant, shared enormous quantities of user data with the National Security Agency without any warrant. Many cyber security strategies mention the need to create such mechanisms but include no detail about what information will be shared, who will decide that the information is shared, what safeguards there are to prevent arbitrary or illegal sharing of information, how undue influence will be avoided, etc. It is important that any such mechanism is well defined and subjected to adequate scrutiny and safeguards.

Safeguards for "metadata" versus actual content?

An additional problem is that many countries seek to apply lesser protections for "metadata" or communications data, than they apply to the actual content of those communications. Communications data refers to, for example, the email address of a sender and recipient of an email, together with the date/time of the message, and the IP addresses of the computers used; or the logs of website addresses visited by a user. It does not include the actual content of the communication.

In many countries this distinction was developed in the offline world where limited information could be garnered from collecting the details of landlines phone calls or the addresses on envelopes. However, given the vast range of activity most Internet users use the Internet for and given the increased ability of the State to collect, store, cross-reference and use this data, it cannot be considered analogous with the same content in an offline world. In fact, it can be argued that metadata can reveal even more than the contents of the communication as it may reveal information that the individual did not realise they were sharing with anyone. The degree to which metadata is or is not different from content, and therefore deserving of different safeguards for access to this data by public authorities is an increasingly important legal question which human rights activists must engage with.

What constitutes valid online protest?

The Internet and digital communications are not only widely used to organise offline protests: the Internet is also a domain within which protests have been conducted. For example, hacktivists from the online activist group "Anonymous" launched distributed denial of service attacks against Paypal, MasterCard and others who stopped servicing payments to Wikileaks in the aftermath of the 2010 release of the diplomatic cables. In January this year, following the suicide of Internet activist Aaron Swartz, Anonymous hackers hacked into the website of the U.S. Department of Justice to protest against what it described as

harsh treatment of Swartz. The hackers defaced the Sentencing Commission site with an alternative video praising Swartz and denouncing the government.

At the moment these is no clear definition of what constitutes legitimate protest in the online domain. In fact, the UK Cyber Security Strategy 2010 identifies politically-motivated hackers as one of the primary perpetrators of cyber security risks, without any discussion about whether such hacking may in certain circumstances constitute legitimate speech. This is particularly obvious when it comes to the prosecution and sentencing patterns. For example, a number of hackers involved in the attacks against Paypal were given hefty prison sentences (including an 18-month sentence). This is a much more severe sentence than a protester in a traditional sit-in would have been likely to receive. Hacktivists are often lumped together with cyber criminals in cyber security strategies, but it is important to distinguish between crimes and actions which can be more accurately defined as an attempt to protest and effect change. By clubbing all hacktivists together with criminals, governments are undermining citizen's right to dissent.

Do we need a demilitarisation of the cyber security debate?

There are signs that some governments have invested in developing so-called “cyber arms” and offensive cyber attacks. These trends are extremely worrying from a human rights perspective: they are likely to lead to a curb on civil liberties as governments argue that curbs are necessary to promote security and “weapons” could be developed that cause real damage to the Internet architecture, undermining individuals from using it and gaining the benefits thereof. This is especially true in an interconnected ecosystem like the Internet where it is impossible to contain the impact of any so-called cyber war.

There have been recent attempts to look at how humanitarian law applies to the online space, for example by the International Group of Experts convened by NATO (The Tallinn Manual). There is a need to also look at how human rights apply in situations of cyber war. However, perhaps even more important is for human rights activists to consider whether we need a cyber arms treaty or even a cyber demilitarisation movement. At present, not a single government has taken a leadership role in de-escalating the cyber arms race, for example by indicating that they will not be the first to strike.

Cyber Security and Internet Governance

At the international level, concerns about cyber security feed into demands from States who want to assert their sovereignty over this new domain. In September 2011, for example, Russia, China, Uzbekistan and Tajikistan submitted a proposal to the United Nations General Assembly for an International Code of Conduct for the Information Society, calling for UN level action on the issue of cyber security. The preamble states that "policy authority for Internet-related public issues is the sovereign right of the States". This was also seen more recently at the World Conference on International Telecommunications in Dubai in December 2012, where governments from around the world had met to renegotiate the International Telecommunications Regulations (ITRs). Many governments, particularly those from developing and transitional countries, sought to establish greater control over the Internet in Dubai by seeking to bring it firmly within the ambit of the ITRs. These attempts were often justified by security concerns and the inability of governments in question to address these adequately within current Internet governance arrangements.

A distributed-governance approach to cyber security

While cyber threats are often real, the current discourse is thus having a variety of negative impacts, moving the Internet governance agenda away from creating an accessible and enabling environment and towards finding new, and increasingly centralised, forms of command and control. A defining feature of the cyber security discourse is the notion of a powerful and benevolent State providing its citizens with security, as it did in the pre-Internet age. But this narrative sits uneasily with the reality of the Internet's nature, which is a global network of information that is to a large extent in the hands of the private sector. Neither threats nor solutions are therefore as easily defined, located or circumscribed as they were in earlier eras. As Ron Deibert has pointed out, where state-based agencies are privileged as lead actors in securing this space, this can then "create awkward privacy concerns in domestic settings while fuelling reciprocal suspicions on an international scale", not in the least because actions of one state seem to affect the sovereignty of others [14].

For this reason, Deibert proposes we move to a distributed approach to cyber security, which relies fundamentally on checks and balances among a variety of actors, both nationally and internationally, so as to avoid the emergence of "unchecked and concentrated political power". In a distributed approach, governance arrangements intentionally accord multiple actors specific roles and responsibilities in the cyber security

[14] Deibert, R. (2012). Dark Side of Cyberspace.

arena, but do so in such a way that no single actors is able to control this arena unless the others agree and collaborate. One of the strengths of such an approach is that it allows us to once again recognise the user as an important actor in this area. Indeed, as threats are fast-changing in the Internet environment, the best defence will often be having informed users who are able to make intelligent decisions; yet in the current governance arrangements, there is little space for this. In addition, by mandating multi-layers of checks and balances, such an approach would be more likely to support human rights.

To be effective, however, this approach also requires a strong commitment to mutual restraint as envisioned under international human rights law. This is required first and foremost on the part of states, who at the moment all too often engage in deliberate manipulation of security weaknesses and threats to their own ends. However, it is also needed on the part of Internet businesses, who possess large amounts of data on Internet users but often handle this in less than transparent ways. In both cases, all policies and practices should be brought in line with human rights standards, and oversight mechanisms should be established to consistently verify that this is indeed the case.

For current debates on global Internet governance and enhanced cooperation, this provides important pointers on the way forward. In the area of cyber security at least, what such conversations should focus on is not a renewal of government control traditional style, but the establishment of networks of governance actors and institutions, both domestically and internationally, who are linked in multiple ways and have a crucial stake in supporting and collaborating with each other.

In some cases, the formalisation of the roles of different actors might require the establishment of new institutions and arrangements. However, such networks would also include existing multistakeholder mechanisms, such as ICANN, that already count as part of their responsibilities particular aspects of cyber security, and could also integrate to a greater extent than is currently the case existing UN mechanisms. For example, the UN Human Rights Council could play a crucial role in conceptualising and developing accountability mechanisms that respond appropriately to the peculiarities of the Internet while at the same time having the protection and promotion of human rights at their core. Each actor would play a crucial, well-defined yet circumscribed role, without being able to dominate the arena. If mutual restraint on the part of governments and businesses is crucial to enhancing cyber security for all, this should not simply be left to the good intentions of these actors. A distributed approach to cyber security

is the way forward because it ensures that the need for restraint is embedded in governance arrangements and institutions.

Conclusion

There is an urgent need for a human rights approach to cyber security. Current cyber security debates suffer from a lack of definitional clarity that allows all initiatives in this area to be overtaken by a sense of crisis, whether or not such a sense is legitimate. In this atmosphere, insufficient efforts are made to establish the exact nature and seriousness of each threat and to investigate the cost of solutions offered and whether they actually counter the problem that they claim to address. In addition, the often problematic role of governments and businesses in contributing to insecurity is hidden from view.

An important reason why this has been allowed to happen is because the approach taken to security is a negative one: security is defined as an absence of harm. In contrast, we propose a positive approach to security that puts people and their ability to be fearless online at the centre. Rather than the disempowering effect of current policies, such an approach would fundamentally empower people, including by substantively scaling back surveillance measures and returning to people their right and ability to protect themselves online. At the heart of such an approach would be the extent to which cyber security measures respect and support the right to privacy and the right to freedom of expression. Though other human rights are relevant too, these are key rights to facilitate people's fearlessness online. By assessing contentious issues and their proposed resolutions against the extent to which they respect and support these rights, important progress could be made.

Finally, this approach relies on governments and businesses agreeing to exercise mutual restraint. In order to institutionalise the principle of restraint, a distributed approach to Internet governance is required, which acknowledges and respects the role of a wide variety of actors and, through a system of checks and balances, ensures that none of these actors can control the field without the collaboration and agreement of the others. Such an approach would be more suited to the realities of the new environment that the Internet has brought about. It would also make it possible to shift the emphasis in cyber security State-centric approaches to ones which are people-centric.