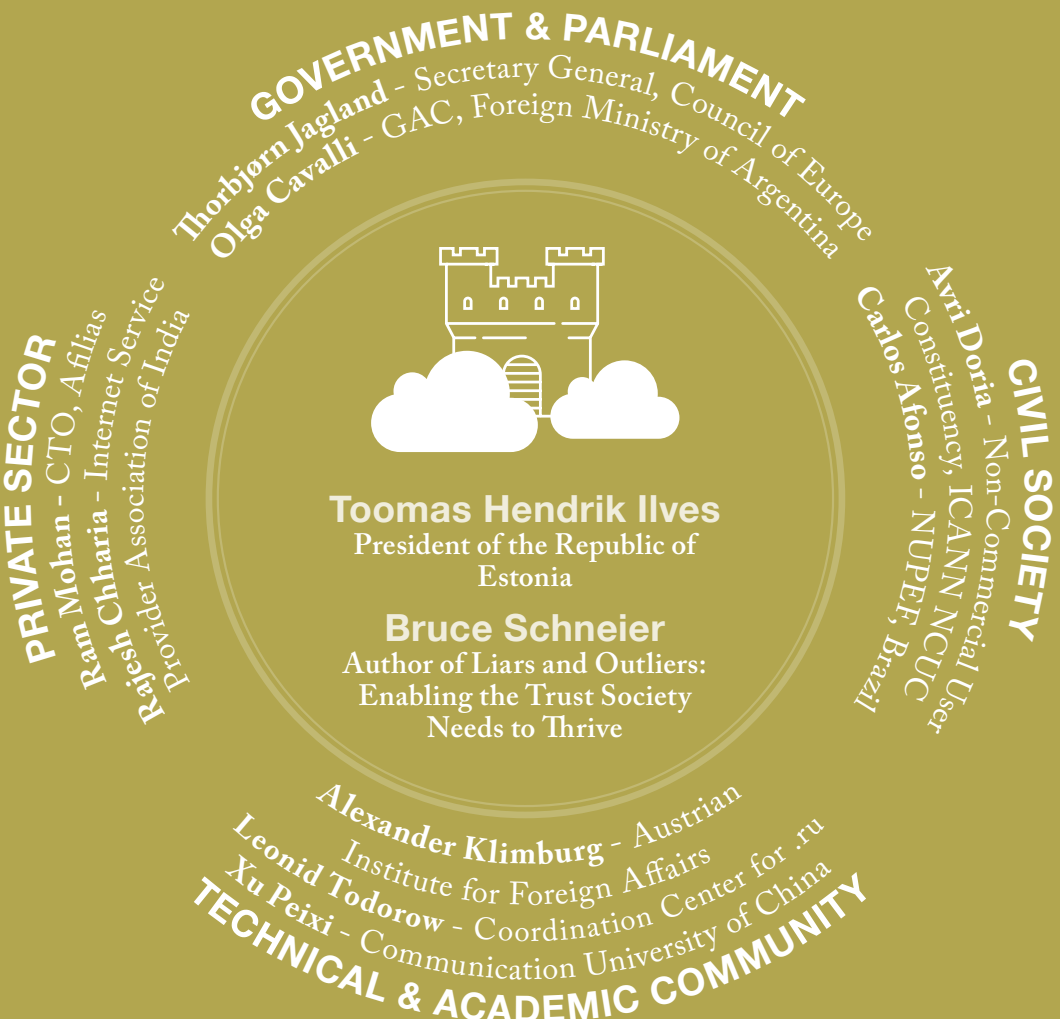
# MIND

MULTISTAKEHOLDER INTERNET DIALOG

CO:LLABORATORY DISCUSSION PAPER SERIES NO. 1

# #6 Internet and Security




*A publication by the Internet & Society Collaboratory*

Editor - Wolfgang Kleinwächter

Internet & Society Co:llaboratory

MIND

MULTISTAKEHOLDER INTERNET DIALOG

CO:LLABORATORY DISCUSSION PAPER SERIES NO. 1

# #6 Internet and Security

BROADENING YOUR **MIND.**

*A publication by the Internet & Society Collaboratory*
Editor · **Wolfgang Kleinwächter**

*1st Edition*
*ISBN 978-3-00-043691-8*

# CONTENT

## RESPONSES CIVIL SOCIETY



## RESPONSES TECHNICAL & ACADEMIC COMMUNITY

# PREFACE

*The Collaboratory Steering Group*
*Dr. Philipp S. Müller, Dr. des. Ulrike Höppner, Martin G. Löhe, Dr. Marianne Wulff, John H. Weitzmann*

In 1775, Benjamin Franklin wrote "they who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety." [1]

We live in a time where our vision of a free and globe-spanning cosmopolitan communications infrastructure - the internet - is being shattered by the exposure of significant instances of secret government surveillance in western liberal democracies, the erosion of privacy as we knew it, the introduction of new tools and practices of censorship on the internet and threats of cyberwarfare, the significance of which we are only beginning to understand. The internet is growing up and facing the similar challenges as other technological advances before. It has entered adolescence, and it is yet unclear how it will turn out when it becomes an adult technology. Now is the crucial time to shape our thinking about how this global infrastructure permeating our societies on all levels should look like when today's children will be the drivers of technological change to come.

The information and communication infrastructure that forms the back-bone of commerce, government, healthcare, civil organizations and entertainment needs to be a reasonably secure and reliable infrastructure and substantial challenges remain: Power outages cause real damage, data loss has potentially far-reaching consequences, criminal intrusion into crucial infrastructure is not easily prevented and systems preserving our digital heritage are in their infancy. Pessimists paint a grim picture of the global threats we face but Benjamin Franklin would warn that if we sacrifice our liberties trying to secure our infrastructure, we would have failed. We need a global debate about the tension between security and freedom and we need to ensure that it is an informed debate about the ways we approach internet regulation, governance and security involving all relevant stakeholders. It took decades to establish forums for the prevention of war and genocide and, imperfect as they may be, they provide important and valuable frameworks. It is now time to build and strengthen our frameworks for shaping the global network infrastructure, making the internet viable for coming decades and preventing a descend into an Orwellian surveillance society as well as the collapse and fragmentation of the global internet.

1 Ascribed to Franklin as as part of his notes for a proposition at the Pennsylvania Assembly, published in Memoirs of the life and writings of Benjamin Franklin (1818).

# INTERNET GOVERNANCE AND CYBERSECURITY

*Prof. Dr. Wolfgang Kleinwächter, Editor*

Cybersecurity is as important as the openness and freedom of the Internet. An insecure cyberspace undermines individual human rights, blocks online businesses and hinders the free exchange of information. And it is bad for innovation and sustainable development. People want to live in a safe environment when they enter the virtual space.

But like everything in life, security has a price. Very often the currency for security on the Internet is not only money, it is also privacy and freedom. Governments argue that they need less data protection and have to limit some individual freedoms in order to provide security. Both security and privacy are important issues. In other words, there is a conflict of values and the big challenge is how to find the right balance in the conflict and define the "right price". If cybersecurity is "overpriced", the costs which come with the reduction of freedom of expression, freedom of association and freedom of movement could have a damaging effect on the Internet economy and society as a whole.

The problem is even more complex because there is no globally accepted definition of what Internet security – or more broadly "cybersecurity" – means in detail. Different people (and governments) have different ideas. For some groups, it is just the technical security of the network, for others cybersecurity means the fight against cybercrime as defined in the Budapest Convention of 2001. And a third group links the concept of cybersecurity primarily to the issue of national security. In this respect, nearly everything people do on the web has a "security dimension".

The Internet is an enabling technology. It enables the good guys to develop and introduce wonderful new services and applications which enhance business opportunities and individual freedoms. But it also enables criminals, warriors, terrorists, vandals, hate preachers, pedophiles and other "bad guys" to do bad things. And with the development of "cyberweapons" the risk of a militarization of cyberspace is growing. As a result, we see more Internet control, surveillance of e-mails and state sponsored cyberespionage, which affect the free and open Internet we have known since the early 1990s.

Historically, this is not new. When the telegraph emerged as a new communication technology in the 19th century, new laws guaranteed the "privacy of correspondence, posts and telecommunications" as enshrined in the Fourth Amendment to the US Constitution and the constitutions of the main European countries. But the laws also allowed the government and law enforcement agencies to intercept private communications for criminal investigations and to protect "national security". This was also reflected in the first international telegraph convention of 1865, in which European governments reserved their right to interfere with, and even stop, telegraph communication in cases where "national security" or "state secrets" were at stake. The same legal mechanism was introduced in the Berlin Radio-Telegraphy Convention of 1906, in the Geneva Broadcasting convention of 1936 and even in the Human Rights Convention of 1966, in which Article 19, paragraph 3 allows governments to limit freedom of expression to protect national security, public order, public health and morals.

The vague definition of national security, public order, morals and state secrets creates slippery territory. It is also an invitation for a broad interpretation. The reality is that if governments see a problem with privacy, freedom of association and freedom of expression, they refer to the principle of "national sovereignty" and define for themselves what the security concerns are to justify censorship or interference into private communication.

In a democratic society, independent courts, including constitutional courts, decide whether a government is misusing its rights and violating other individual or institutional rights and freedoms. Not everything governments want to do to "enhance security" is in accordance with recognized human rights and constitutional norms. Cases from the US in the 1970s, such as the Pentagon Papers or the Watergate scandal, where individuals published "state secrets" which were seen by the acting US government as a threat to national security, were brought to court. And in the case of the Pentagon Papers, the US Supreme Court decided in favor of the freedom of the press and against the government. The New York Times continued to publish the Pentagon Papers and after the Watergate scandal, President Nixon had to resign.

In less democratic societies, where the rule of law is disregarded and no independent court system can stop a government doing the wrong thing, the situation is much worse. Governments simply

do what they think is needed. This opens the door for all kinds of misuse in the name of "security". From the Spanish Inquisition to the East German Stasi, a need for surveillance mechanisms has always been justified to protect "national security" and to find the "bad guys" who want to remove the government or damage the reputation of their religious or political leaders.

In other words, the conflict between "security" and "privacy and freedom of expression" is not new, but cyberspace has moved this conflict to a new level. It is not a national issue anymore; the removal of the barriers of time and space has made this a global problem.

Crime and terrorist attacks in cyberspace are taking place in real time and regardless of borders. But our legal procedures are defined within a national jurisdiction. Fighting against the "bad guys" online effectively means that one has to go beyond national borders. This can be done via enhanced cooperation among governments and their law enforcement institutions. This is time consuming and needs a political will to agree on common values, which is quite often unrealistic to achieve.

An alternative is to use new surveillance technologies and to go beyond national borders without the consent of a third party or the affected national jurisdiction. This certainly has a number of legal implications which need further investigation. In the hunt for terrorists, is it justified to break privacy and data protection laws in third countries? Is intercepting undersea fiber optic cables, which are used for private communication, allowed because the interception points are outside of a national jurisdiction and the issue is not regulated in the UN Law of the Sea Convention of 1982? What about intercepting satellite communications, which is becoming more important with further cloud computing and the Internet of Things? And who monitors the surveillants and controls the controllers? Who defines what level of surveillance is needed to enhance the security of people and countries? And finally, is it possible to bring the legally required surveillance under the rule of law and in line with national constitutional rights and freedoms, as well as with international legal norms, as enshrined in the Charter of the United Nations?

There are now proposals on the table to add a "Privacy Protocol" to the UN Covenant on Civil and Political Rights of 1966. The NATO Center of Excellence in Tallinn, Estonia, has published a manual in which it is investigated how existing international law, including international hu-

manitarian law, is applicable to a cyberwar. Discussions on cybersecurity and cyberwar have started in the OSCE and in the 1st Committee of the UN General Assembly. The UN has established a so-called Group of Governmental Experts (GGE) to find out what can be done and whether one can start with confidence building measures in cyberspace to find a balanced solution which contributes to enhancing security in the online world. The US government has entered into bilateral consultations with a number of governments, including China, Russia and Germany.

The disclosure of the NSA PRISM program and other online activities of intelligence agencies has pushed the discussion to a new level. The risk is now that we could see not only a militarization of cyberspace, but also something that could be similar to the nuclear arms race during the Cold War of the second half of the 20th century. Will competing governments try to develop their own technologies for global surveillance and spy as much as possible on what is going on in third countries? This would certainly undermine the trust in Internet communication and would have negative effects on the global Internet economy and individual freedoms. This would be a bad choice.

The Brazilian President Dilma Rousseff raised these issues in her speech at the 68th Session of the UN General Assembly in New York on September 24, 2013 when she said: "Information and telecommunication technologies cannot be the new battlefield between States. Time is ripe to create the conditions to prevent cyberspace from being used as a weapon of war, through espionage, sabotage and attacks against systems and infrastructure of other countries." She proposed "the establishment of a civilian multilateral framework for the governance and use of the Internet" which should be based, inter alia, on "freedom of expression, privacy of the individual and respect for human rights", "transparency", "universality, "cultural diversity" and network neutrality under the full participation of all stakeholders. [1]

The question is whether the multistakeholder approach to Internet governance offers an alternative for discussing and enhancing security in cyberspace. Could this become a helpful tool which

1 http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf

would enable governments to find the right balance to do what they have to do to keep the Internet secure by respecting individual rights and freedoms? The non-governmental stakeholders obviously have a great role to play.

Private sector corporations, such as Google, Facebook and others, have already started to bring more transparency into their relationships with governments by disclosing data requests coming from governmental agencies. The technical community, such as the IETF, has started discussions on how standards and protocols can be developed to make individual communication more resistant against foreign or domestic surveillance. And civil society is coming together to write statements and protest in the streets. In Berlin, more than 20,000 people protested against surveillance in early September 2013. Recent statements by organizations including the Electronic Frontier Foundation, Human Rights Watch and the Internet Society have shown that people do not accept governmental wrongdoing, neither from democratic nor from non-democratic governments. The Internet Society President and CEO, Lynn St. Amour, said as a response to the NSA activities on September 10th, 2013: "If true, these reports describe government programs that undermine the technical foundations of the Internet and are a fundamental threat to the Internet's economic, innovative and social potential. Any systematic, state-level attack on Internet security and privacy is a rejection of the global, collaborative fabric that has enabled the Internet's growth to extend beyond the interests of any one country."

In 2011, the UN Human Rights Council unanimously affirmed that "the same rights that people have offline must also be protected online [so has the Collaboratory's 5th expert initiative], in particular freedom of expression". This means that the offline right for private communication to be protected against unauthorized external inspection and investigated only under strict legally defined circumstances, based on evidence of wrongdoing and under the inclusion of a neutral third party, is also relevant for the online world.

A lot of things relating to cybersecurity will need to be discussed in the years ahead of us. One place for discussion could be the Internet Governance Forum (IGF). This is a place where all stakeholders are involved. And it would certainly be useful if governments were ready to discuss

issues related to cybersecurity not only in their own circles, but also share their ideas, needs and positions with other stakeholders on a global level. While it is understandable that not everything can be open to the public and governments (as individuals) need their "secrets", a lot more transparency can be brought to the issue, in particular with regard to procedures.

We hope that MIND 6 – which will be distributed to all participants of the 8th Internet Governance Forum (IGF) in Bali in October 2013 – will make a contribution to this discussion. You are invited to continue this debate online at: http://www.collaboratory.de/

# *Propositions*

TOOMAS HENDRIK ILVES
*President of the Republic of Estonia*

BRUCE SCHNEIER
*Cryptographer and Computer Security Specialist*

# CYBERSECURITY: A VIEW FROM THE FRONT

*Toomas Hendrik Ilves, President of the Republic of Estonia*

The changes in the digital world today represent a dramatically sped-up version of the changes the world underwent in a century of industrialization. It is a paradigm transformation of our world: notions of a nation's size, wealth, power, military might, population and GDP mean something altogether different from what they meant a generation ago.

These relations are in constant flux, and old assumptions no longer hold. Today, a small, poor East European country can be a world leader in e-governance and cybersecurity.

In February, the United Nations praised Estonia's e-Annual Report system, by which entrepreneurs can submit annual reports electronically, as the "best of the best" e-Government application of the past decade. Last autumn, Freedom House ranked Estonia first in Internet freedom for the third year in a row (the United States and Germany were second and third).

At the same time, Estonia is also remembered as the first publicly known target of politically motivated cyberattacks in April 2007, which inundated the websites of Parliament, banks, ministries, television stations and other organizations.

Disruptive as the attacks were, they were by today's standards primitive, consisting of "distributed denial of service" attacks (DDoS), which essentially overload servers with signals from hijacked, hacker-controlled PCs. Six years later, as computing power and IT dependency have increased hugely, cyberattacks are far more sophisticated and our vulnerabilities are far greater.

Yet those attacks were a blessing – Estonia took cybersecurity seriously earlier than most. In 2008, NATO opened its Cooperative Cyber Defense Center of Excellence, to enhance NATO's cyberdefense capability, in Tallinn.

Cybersecurity needs to be taken seriously by everyone. We continue to think of cyberthreats in military or classical warfare terms, when in fact cyber can simply render the military paradigm irrelevant. The whole information and communication technologies (ICT) infrastructure must be regarded as an "ecosystem" in which everything is interconnected. It functions as a whole; it must be defended as a whole.

Today, almost everything we do depends on a digitized system of one kind or another. Our critical infrastructure – our electrical, water or energy production systems and traffic management – essentially interacts with, and cannot be separated from, our critical information infrastructure: private Internet providers, lines of telecommunications and the Supervisory Control and Data Acquisition (Scada) systems that run everything from nuclear power plants to delivery of milk to our supermarkets.

Understanding that cybersecurity means defending the entirety of our societies, we need to re-examine many assumptions of security. In cyberwarfare, it is much harder to identify the attacker, and therefore to know how to retaliate.

In a modern digitized world it is possible to paralyze a country without attacking its defense forces: the country can be ruined by simply bringing its Scada systems to a halt. To impoverish a country one can erase its banking records. The most sophisticated military technology can be rendered irrelevant. In cyberspace, no country is an island.

This requires rethinking some of our core philosophical notions of modern society: the relations between

the public and private spheres, between privacy and identity.

At a time when the greatest threats to our privacy and the security of our data come from criminal hackers and foreign countries (often working together), we remain fixed on the idea that Big Brother, our own government, is the danger.

This may have been true in the past, when only national governments had the ability to monitor citizens. Today, as we know, a single hacker can access the most intimate details of your digital and nondigital life, your finances and your correspondence.

This is a clear case of market failure. A bank that builds identity theft and fraud into the cost of doing business is an example of market failure. A power company that treats a cyber-induced power outage as an act of God, no different from a tornado or earthquake, demonstrates market failure.

If the private sector is unwilling to take the necessary steps to guarantee the integrity of its online activities, the government must step in to fulfill its most fundamental task – to ensure the security of its citizens; that is, to provide them with a secure identity.

Identity lies at the core of security online. Virtually all breaches of computer security involve a fake identity, be it stealing a credit card number or accessing the internal documents of the European Commission. A three-digit security code on the back of a credit card does not provide you with a secure identity, nor does an ordinary computer password. The fundamental question is whether you can be sure the person you interact with online is who he claims he is.

The key to all online security is a secure online identification system. But a nebulous fear of an imagined Big Brother prevents citizens in many places from adopting a smart-chip-based access key that would afford them secure online transactions.

In Estonia, the government has become the guarantor of secure transactions online, while identity is authenticated by a body independent of the government. We use a two-factor identification system in which the ID is protected by both a chip and a password. A binary key or public key infrastructure guarantees securely encrypted transfer of information. Thus far, our system has proved secure. Even during the DDoS attacks of 2007, our digital government system remained online and intact.

Precisely because we offer a verifiable and reliable identification system, Estonia has gone further than any other country in investing in digitizing the basic processes of society. A quarter of the electorate votes online, 95 percent of tax returns are done online and 95 percent of prescriptions are filled online.
By the end of 2012, Estonians had given more than a hundred million digital legal signatures. Citizens, as legal owners of their own data, have access to their digital medical and dental records. And we have more and more e-services available every year.

In the future, we hope to connect our digital services and make them interoperable with our neighbors in Northern Europe. In the longer run, we're looking toward uniting systems in all of Europe. Ultimately, government data will move across borders as freely as e-mail and Facebook and follow the international flows of commerce and trade.

The job of **cybersecurity** is to enable a globalized economy based on the **free** movement of people, goods, services, capital and ideas. This can only be accomplished if identities are secure.

Undoubtedly the most effective means by which our societies could be safeguarded from cyberattacks would be to roll back the clock – to go back to the pen, typewriter, paper and mechanical switch. We should give up on mobile phones, iPads, online banking, social media, Google searches – everything we have become accustomed to in the modern world. But that won't happen.

Cybersecurity is not just a matter of blocking bad things a cyberattack can do; it is protecting all the good things that cyberinsecurity can prevent us from doing. Genuine cybersecurity should not be seen as an additional cost, but as an enabler, guarding our entire digital way of life.

# POWER IN THE AGE OF THE FEUDAL INTERNET

*Bruce Schneier, Cryptographer and Computer Security Specialist*
*Author of Liars and Outliers: Enabling the Trust Society Needs to Thrive*

We're in the middle of an epic battle for power in cyberspace. On one side are the nimble, unorganized, distributed powers such as dissident groups, criminals, and hackers. On the other side are the traditional, organized, institutional powers such as governments and large multinational corporations. During its early days, the Internet gave coordination and efficiency to the powerless. It made them powerful, and seem unbeatable. But now the more traditional institutional powers are winning, and winning big. How these two fare long-term, and the fate of the majority of us that don't fall into either group, is an open question – and one vitally important to the future of the Internet.

In its early days, there was a lot of talk about the "natural laws of the Internet" and how it would empower the masses, upend traditional power blocks, and spread freedom throughout the world. The international nature of the Internet made a mockery of national laws. Anonymity was easy. Censorship was impossible. Police were clueless about cybercrime. And bigger changes were inevitable. Digital cash would undermine national sovereignty. Citizen journalism would undermine the media, corporate PR, and political parties. Easy copying would destroy the traditional movie and music industries. Web marketing would allow even the smallest companies to compete against corporate giants. It really would be a new world order.

Some of this did come to pass. The entertainment industries have been transformed and are now more open to outsiders. Broadcast media has changed, and some of the most influential people in the media have come from the blogging world. There are new ways to run elections and organize politically. Facebook and Twitter really did help topple governments.

But that was just one side of the Internet's disruptive character. Today, the traditional corporate and government power is ascendant, and more powerful than ever.

On the corporate side, power is consolidating around both vendor-managed user devices and large personal-data aggregators. It's a result of two current trends in computing. First, the rise of cloud computing means that we no longer have control of our data. Our e-mail, photos, calendar, address book, messages, and documents are on servers belonging to Google, Apple, Microsoft, Facebook, and so on. And second, the rise of vendor-managed platforms means that we no longer have control of our computing devices. We're increasingly accessing our data using iPhones, iPads, Android phones, Kindles, ChromeBooks, and so on. Even Windows 8 and Apple's Mountain Lion are heading in the direction of less user control.

I have previously called this model of computing feudal. Users pledge allegiance to more powerful companies who, in turn, promise to protect them from both sysadmin duties and security threats. It's a metaphor that's rich in history and in fiction, and a model that's increasingly permeating computing today.

Feudal security consolidates power in the hands of the few. These companies act in their own self-interest. They use their relationship with us to increase their profits, sometimes at our expense. They act arbitrarily. They make mistakes. They're deliberately changing social norms. Medieval feudalism gave the lords vast powers over the landless peasants; we're seeing the same thing on the Internet.

It's not all bad, of course. Medieval feudalism was a response to a dangerous world, and depended on hierarchical relationships with obligations in both directions.

We – especially those of us who are not technical – like the convenience, redundancy, portability, automation, and shareability of vendor-managed devices. We like cloud backup. We like automatic updates. We like it that Facebook just works – from any device, anywhere.

Government power is also increasing on the Internet. Long gone are the days of an Internet without borders, and governments are better able to use the four technologies of social control: surveillance, censorship, propaganda, and use control. There's a growing "cyber sovereignty" movement that totalitarian governments are embracing to give them more control – a change the US opposes, because it has substantial control under the current system. And the cyberwar arms race is in full swing, further consolidating government power.

In many cases, the interests of corporate and government power are aligning. Both corporations and governments want ubiquitous surveillance, and the NSA is using Google, Facebook, Verizon, and others to get access to data it couldn't otherwise. The entertainment industry is looking to governments to enforce their antiquated business models. Commercial security equipment from companies like BlueCoat and Sophos is being used by oppressive governments to surveil and censor their citizens. The same facial recognition technology that Disney uses in its theme parks also identifies protesters in China and Occupy Wall Street activists in New York.

What happened? How, in those early Internet years, did we get the future so wrong?

The truth is that technology magnifies power in general, but the rates of adoption are different. The unorganized, the distributed, the marginal, the dissidents, the powerless, the criminal: they can make use of new technologies faster. And when those groups discovered the Internet, suddenly they had power. But when the already powerful big institutions finally figured out how to harness the Internet for their needs, they had more power to magnify. That's the difference: the distributed were more nimble and were quicker to make use of their new power, while the institutional were slower but were able to use their power more effectively.

So while the Syrian dissidents used Facebook to organize, the Syrian government used Facebook to identify dissidents.

All isn't lost for distributed power, though. For institutional power the Internet is a change in degree, but for distributed power it's a change of kind. The Internet gives decentralized groups – for the first time – access to coordination. This can be incredibly empowering, as we saw in the SOPA/PIPA debate, Gezi, and Brazil. It can invert power dynamics, even in the presence of surveillance censorship and use control.

There's another more subtle trend, one I discuss in my book Liars and Outliers. If you think of security as an arms race between attackers and defenders, technological advances – firearms, fingerprint identification, lockpicks, the radio – give one side or the other a temporary advantage. But most of the time, a new technology benefits the attackers first.

We saw this in the early days of the Internet. As soon as the Internet started being used for commerce, a new breed of cybercriminal emerged, immediately able to take advantage of the new technology. It took police a decade to catch up. And we saw it on social media, as political dissidents made quicker use of its organizational powers before totalitarian regimes were able to use it effectively as a surveillance and propaganda tool. The distributed are not hindered by bureaucracy, and sometimes not by laws or ethics. They can evolve faster.

This delay is what I call a "security gap". It's greater when there's more technology, and in times of rapid technological change. And since our world is one in which there's more technology than ever before, and a greater rate of technological change than ever before, we should expect to see a greater security gap than ever before. In other words, there will be an increasing time period where the nimble distributed power can make use of new technologies before the slow institutional power can make better use of those technologies.

It's quick vs. strong. To return to medieval metaphors, you can think of a nimble distributed power – whether marginal, dissident, or criminal – as Robin Hood. And you can think of ponderous institutional power

– both government and corporate – as the Sheriff of Nottingham.

So who wins? Which type of power dominates in the coming decades?

Right now, it looks like institutional power. Ubiquitous surveillance means that it's easier for the government to round up dissidents than it is for the dissidents to anonymously organize. Data monitoring means it is easier for the Great Firewall of China to block data than it is to circumvent it. And as easy as it is to circumvent copy protection schemes, most users can't do it.

This is largely because leveraging power on the Internet requires technical expertise, and most distributed power groups don't have that expertise. Those with sufficient technical ability will be able to stay ahead of institutional power. Whether it's setting up your own e-mail server, effectively using encryption and anonymity tools, or breaking copy protection, there will always be technologies that are one step ahead of institutional power. This is why cybercrime is still pervasive, even as institutional power increases, and why organizations like Anonymous are still a social and political force. If technology continues to advance – and there's no reason to believe it won't – there will always be a security gap in which technically savvy Robin Hoods can operate.

My main concern is for the rest of us: everyone in the middle. These are people who don't have the technical ability to evade either the large governments and corporations that are controlling our Internet use, or the criminal and hacker groups who prey on us. These are the people who accept the default configuration options, arbitrary terms of service, NSA-installed back doors, and the occasional complete loss of their data. In the feudal world, these are the hapless peasants. And it's even worse when the feudal lords – or any powers – fight each other. As anyone watching Game of Thrones knows, peasants get trampled when powers fight: when Facebook, Google, Apple, and Amazon fight it out in the market; when the US, EU, China, and Russia fight it out in geopolitics; or when it's the US vs. the terrorists or China vs. its dissidents.

The abuse will only get worse as technology continues to advance. In the battle between institutional power and distributed power, more technology means more damage. Cybercriminals can rob more people more quickly than criminals who have to physically visit everyone they rob. Digital pirates can make more copies of more things much more quickly than their analog forebears. And 3D printers mean that the data use restriction debate now involves guns, not movies. It's the same problem as the "weapons of mass destruction" fear: terrorists with nuclear or biological weapons can do a lot more damage than terrorists with conventional explosives.

It's a numbers game. Very broadly, assume there's a particular crime rate society is willing to tolerate. With historically inefficient criminals, we were willing to live with some percentage of criminals in our society. As technology makes each individual criminal more powerful, the percentage we can tolerate decreases. This is essentially the "weapons of mass destruction" debate: as the amount of damage each individual terrorist can do increases, we need to do increasingly more to prevent even a single terrorist success.

The more destabilizing the technologies, the greater the rhetoric of fear, and the stronger institutional power will get. This means even more repressive security measures, even if the security gap means that such measures are increasingly ineffective. And it will squeeze the peasants in the middle even more.

Without the protection of feudal lords, we're subject to abuse by criminals and other feudal lords. Also, there are often no other options but to align with someone. But both these corporations and the government – and sometimes the two in cahoots – are using their power to their own advantage, trampling on our rights in the process. And without the technical savvy to become Robin Hoods ourselves, we have no recourse but to submit to whatever institutional power wants.

So what happens as technology increases? Is a police state the only effective way to control distributed power and keep our society safe? Or do the fringe elements inevitably destroy society as technology increases their power? Probably neither doomsday scenario will come to pass, but figuring out a stable middle ground is hard.

These questions are complicated, and dependent on future technological advances that we cannot predict. But they are primarily political questions, and any solutions will be political.

In the short term, we need more transparency and oversight. The more we know of what institutional powers are doing, the more we can trust that they are not abusing their authority. We have long known this to be true in government, but we have increasingly ignored it in our fear of terrorism and other modern threats. This is also true for corporate power. Unfortunately, market dynamics will not necessarily force corporations to be transparent; we need laws to do that. The same is true for decentralized power; transparency is how we will differentiate political dissidents from criminal organizations.

Oversight is also critically important, and is another long-understood mechanism for checking power. This can be a combination of things: courts that act as third-party advocates for the rule of law rather than rubber-stamp organizations, legislatures that understand the technologies and how they affect power balances, and vibrant public-sector press and watchdog groups that analyze and debate the actions of those wielding power.

Transparency and oversight give us the confidence to trust institutional powers to fight the bad side of distributed power, while still allowing the good side to flourish. For if we are going to entrust our security to institutional powers, we need to know they will act in our interests and not abuse that power. Otherwise, democracy fails.

In the longer term, we need to work to reduce power differences. The key to all of this is access to data. On the Internet, data is power. To the extent the powerless have access to it, they gain in power. To the extent that the already powerful have access to it, they further consolidate their power. As we look to reducing power imbalances, we have to look at data: data privacy for individuals, mandatory disclosure laws for corporations, and open government laws.

Medieval feudalism evolved into a more balanced relationship in which lords had responsibilities as well as rights. Today's Internet feudalism is both ad-hoc and one-sided. Those in power have a lot of rights, but increasingly few responsibilities or limits. We need to rebalance this relationship. In medieval Europe, the rise of the centralized state and the rule of law provided the stability that feudalism lacked. The Magna Carta first forced responsibilities on governments and put humans on the long road toward government by the people and for the people. In addition to re-reigning in government power, we need similar restrictions on corporate power: a new Magna Carta focused on the institutions that abuse power in the 21st century.

Today's Internet is a fortuitous accident: a combination of an initial lack of commercial interests, government benign neglect, military requirements for survivability and resilience, and computer engineers building open systems that worked simply and easily. Corporations have turned the Internet into an enormous revenue generator, and they're not going to back down easily. Neither will governments, which have harnessed the Internet for political control.

We're at the beginning of some critical debates about the future of the Internet: the proper role of law enforcement, the character of ubiquitous surveillance, the collection and retention of our entire life's history, how automatic algorithms should judge us, government control over the Internet, cyberwar rules of engagement, national sovereignty on the Internet, limitations on the power of corporations over our data, the ramifications of information consumerism, and so on.

This won't be an easy period for us as we try to work these issues out. Historically, no shift in power has ever been easy. Corporations have turned our personal data into an enormous revenue generator, and they're not going to back down. Neither will governments, who have harnessed that same data for their own purposes. But we have a duty to tackle this problem.

Data is the pollution problem of the information age. All computer processes produce it. It stays around. How we deal with it -- how we reuse and recycle it, who has access to it, how we dispose of it, and what laws regulate it -- is central to how the information age functions. And I believe that just as we look back at the early decades of the industrial age and wonder how society could ignore pollution in their rush to build an industrial world, our

grandchildren will look back at us during these early decades of the information age and judge us on how we dealt with the rebalancing of power resulting from all this new data.

I can't tell you what the result will be. These are all complicated issues, and require meaningful debate, international cooperation, and innovative solutions. We need to decide on the proper balance between institutional and decentralized power, and how to build tools that amplify what is good in each while suppressing the bad.

RESPONSES

# *Government and Parliament*

THORBJØRN JAGLAND
*Secretary General, Council of Europe*

OLGA CAVALLI
*Governmental Advisory Committee (GAC) member of ICANN*
*Senior Advisor Foreign Ministry of Argentina*

# PROTECTING YOU AND YOUR RIGHTS IN CYBERSPACE: MINIMISING THE RISKS, MAXIMISING THE FREEDOM

*Thorbjørn Jagland, Secretary General, Council of Europe*

Cybercrime is a major threat that affects the rights and the security of millions of people and the security of critical information infrastructure in countries worldwide. Governments, therefore, have the positive obligation to protect people against cybercrime, including through criminal justice and law enforcement measures. They need to criminalise offences against and by means of computers, but also provide law enforcement with investigative powers to secure electronic evidence and to engage in efficient international cooperation. Law enforcement powers may include the real-time collection of traffic data or the interception of content data. Law enforcement will also need to cooperate with private sector entities to obtain electronic evidence. However, such measures are to be applied only in specified criminal investigations, they are subject to rule of law safeguards and they need to meet data protection requirements. The more intrusive the measure, the stronger the conditions and safeguards.

Such a criminal justice response to cybercrime is very different from the type of mass surveillance reported in the media. The prevention and control of cybercrime does not justify, and does not need, mass surveillance. Governments – in cooperation with other stakeholders – should be able to take on cybercrime in a way that protects you and your rights while bringing offenders to justice. With the Budapest Convention on Cybercrime, we have an international framework for such an approach, the finality of which is to contribute to human rights and the rule of law in cyberspace.

Action against cybercrime contributes to cybersecurity. The aim of cybersecurity is to enhance the security, resilience, reliability and trust in information and communication technologies. Without cybersecurity a thriving information society would not be possible. Measures on cybercrime and cybersecurity may relate to different concepts, but they are complementary in that both include as key objectives the protection of the confidentiality, integrity and availability of computer data and systems.

Here is where cybersecurity, the prevention and control of cybercrime and the protection of human rights converge. With much of our private and most intimate life taking place on computer systems and stored in the form of digital data, the protection of the confidentiality, integrity and availability of computer data and systems is essential to protect our fundamental rights. This includes the right to private life and other human rights as defined under the European Convention on Human Rights, the Second United Nations Covenant and other international treaties.

The protection of individuals with regard to the automatic processing of data contributes to the respect for their rights and fundamental freedoms, and in particular their right to privacy. Threats to data protection and privacy are acute where vast quantities of personal data flow in digital environments. We need to ensure that more and more countries around the globe commit to strong data protection principles and enact the necessary legislation. Convention 108 of the Council of Europe on the protection of individuals with regard to the processing of personal data should be relevant to any country, in particular now that it is undergoing a process of modernisation.

Moreover, the integrity, universality and openness of the Internet are essential for guaranteeing the right to freedom of expression and access to information regardless of frontiers. The Internet has public service value as individuals and communities around the globe rely on it for their everyday activities, to exercise their fundamental rights and freedoms and have the legitimate

expectation that the Internet will be accessible, secure and affordable. Therefore, the Council of Europe member states have agreed to Internet governance principles which adopt a human rights approach and to a commitment to co-operate with each other to do no harm and preserve the Internet.

The protection of human rights, cybersecurity and action on cybercrime are thus complementary and should go hand in hand.

At the same time, cyberspace is now of strategic importance and is considered a matter of national interest by many governments. National policies thus define cybersecurity as a matter of national security not only to protect the information technology infrastructure, but also the digital economy and the economic well-being of their country. This national security logic on the one hand, and the technical possibility to intercept data flows on the other, may tempt governments to engage in mass surveillance.

We need to be realistic. External and internal security are both essential to protect the interests and values of a State. Effective intelligence and security services are necessities for governments. However, the exceptional powers that security services enjoy carry the risk of abuse of State power. In a democratic society, the activities of security services – in particular those that interfere with the rights of individuals – must, therefore, meet a number of conditions. For example, they must be prescribed by law, and necessary in a democratic society. Those affected must have recourse to effective remedies, and security services must be subject to effective accountability, oversight and control. In short, national security does not legitimise boundless information gathering and surveillance.

Further information and analysis is needed to confirm whether the practices reported in recent weeks meet these conditions, or whether they violate privacy, data protection regulations and other fundamental rights, or amount to cybercrime. If so, they would undermine the very security, trust and confidence necessary for a flourishing, free and open Internet.

# SECURITY AND INTERNET GOVERNANCE, EDUCATION IS THE KEY

*Dr. Olga Cavalli, Governmental Advisory Committee (GAC) member, ICANN*
*Senior Advisor Foreign Ministry of Argentina*

For several years since the creation of the TCP/IP protocol and since the establishment of its early structure, the Internet grew and consolidated before becoming a major communication platform as we know it today. It is an essential tool for allowing our societies to produce find and share any kind of information from any place of the world which is connected to it, and it is the basis of what is called "The Information Society".

The Internet is today highly relevant for communications and businesses in all countries of the world and it also is a key tool for development. The Internet is growing continually, not only in developed countries but also in developing economies, and at the same time the challenges related to Internet security are witnessing a rise as different types of cybercrimes proliferate.

In a highly connected world, all users know that ICTs offer great advantages and are great tools for working and learning, but at the same time there are several security challenges related to this global connectivity. During the last years, illicit cyber activities have grown and they have become a problem for all types of users, whether individuals, corporations or governments.

The different types of cyber attacks and the damages that they can cause show how important education and awareness among the Internet community is. Moreover, differences among the developed and the developing world mean that not all governments have detailed and complete information about what is happening in relation to cyber security and cyber attacks. As shown in the report "Latin American and Caribbean Cyber Security Trends and Government Responses" governments noted an increase in the frequency of cyber incidents during 2012 compared with the previous year; the same study shows that most states did not differentiate between the types or severity of the cyber incidents they reported.[1]

Information shared among governments and other stakeholders, seems to be the right way to face these increasing security challenges. At the same time collaboration among stakeholders at all levels is one of the most important and challenging steps forward, as no problem can be solved in the Internet if it is taken on by only one stakeholder. The multistakeholder model provides the space for sharing experiences and the Internet Governance Forum is an important platform for exchanging knowledge on an equal footing basis. The regional and national IGFs also play an important role in this respect.

Several countries have established alert centers called CSIRTs (Computer Security Incident Response Team) as part of their security infrastructure. Unfortunately, however, there are still a number of countries that have not yet put in place this important tool for a more secure Internet infrastructure. As shown on the global Forum for Incident Response and Security Teams web page, there are still members of this association that are lacking national alert centers, making them more vulnerable to cyber attacks.[2]

Cyber security attacks can potentially cause far-reaching damage to the public and private sectors, to national security, to companies, and to the competitiveness of a country, among many other problems. Eventssuch as these must be avoided, but none of them can be faced or solved by only one stakeholder. On the contrary, having a collaborative and multistakeholder perspective is crucial to our ability to face this challenge.

1 www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-res

2 www.first.org/members/map

For developing countries, the lack of alert centers is only one of many problems. Another is the sheer pace of technological change, which makes it difficult for local regulations and rules to adapt to and reflect those changes. Furthermore, these countries are in need of skilled IT professionals, but their own professionals often emigrate to developed economies that usually pay more for their professional knowledge and skills than their own community. This is a problem for many countries that invest a considerable amount of resources in training these professionals.

There is no single answer to these challenges, but there are some steps that, especially in developing countries, can be taken in order to be stronger when facing cyber security attacks. One of these steps is coordination, each region should make best efforts to coordinate activities and exchange experiences and information to avoid or warn against cyber attacks. Those countries that have experience in establishing and managing an alert center or CSIRT should share this knowledge with those that do not have one and are in the same region. Travelling shorter distances and sharing the same language and cultural similarities always helps in terms of capacity building.

Education, outreach and training are also essential elements that will surely help all developing economies. Creating learning spaces that promote debate in a multistakeholder environment are of great importance. Not all government employees can go to the Internet Governance Forum, but many of them can be part of a capacity building activity that enhances their skills and creates interest to learn and investigate in more detail some aspects of ICTs, Internet and Internet Governance.

Many of the training activities built upon a multistakeholder approach are focused on Internet and Internet Governance, but address these topics from a holistic perspective. Bringing together experts from different backgrounds and professions is the best way to create a basic ground of knowledge for all experts edealing with Internet security challenges on a daily basis.

The Organization of American States has developed a full virtual online training course on Internet Governance that also focusses on security. The course is based on fellowships granted by the OAS and has been developed in Spanish; an English version will be available as of 2014.[3] ISOC also offers fellowships for the online training program called Next Generation Leaders.[4]

The schools on Internet Governance are a great example of global multistakeholder cooperation for training in Internet Governance, including security. The European School on Internet Governance, Euro-SSIG, brings together fellows and well-known academics and experts from all over the world, who teach in a multistakehloder environment. Organized every year in Meissen, Germany, it started in 2007.[5]

In Latin America the South School on Internet Governance, SSIG, has been established since 2009 and takes place in a different Latin American or Caribbean country each year. This school has come to the attention of governments from the regions, who have found that the SSIG is well-positioned to train their experts, as well as students from the region and abroad.[6] The SSIG rotates among countries and has so far been organized in Buenos Aires, Sao Paulo, Mexico, Bogotá and Panama. There is also an African School on Internet Governance that started this year in Durban. South Africa.

This holistic and multistakeholder approach is also important for university teachers. Sometimes universities work in knowledge silos, for example engineering or informatics faculties usually focus on high technical training, but there is a lack of understanding of public policy related with technology. In a similar way, law schools do not usually understand the basic concepts related with technology and some difficulties may arise once there is a need to establish regulations related to the ICT infrastructure of the Internet itself.

Another important issue to achieve is balance, balance between security and censorship. As it has been said before, new challenges are arising in the Internet era

3 www.oas.org/fms/Announcement.aspx?id=357&Type=2&Lang=spa

4 www.internetsociety.org/what-we-do/leadership-programmes/next-generation-leaders-ngl-programme

5 European School on Internet Governance www.euro-ssig.eu

6 South School on Internet Governance www.gobernanzainternet.org

and in the digital economy as new services are constantly being developed; there are new platforms and new ways of interaction between users, in relation to content, their work, their universities, and their families. The overwhelming amount of data that we are all producing, needs to be stored, cared, managed, secured, copied and protected. Governments must protect the information while at the same time protecting the right to communicate, and there is a fine line between security and censorship. Every community has the right to protect t heir culture as it is reflected in digital content on the Internet, but this protection should not prevent others from communicating using the same technology platform.

All the information and the innovation that is generated today by the Internet would not exist if the concept of openness had not been present from the very beginning and if it were not preserved until today. Perhaps the big challenge is not only finding the right balance between regulation and free flow of information, but, more importantly, avoiding any regime that would inhibit the ability of the users to communicate, of the technology providers to continue enabling access, of service providers to offer new services, of academics to conduct research. Security is an increasingly conflicting element with all these desired freedoms on the Internet.

Regulations play an important role in shaping services and defining the way the Internet functions. All parties need to be heard and considered. Finding the right balance seems to be a difficult challenge. And this is precisely why dialogue and the exchange of information within a multistakeholder environment is so important. Indeed, it is the only way to move forward and find practical ideas and solutions to the diverse problems brought about by the open structure of the Internet, cyber security and freedom of expression.

# *Private Sector*

RAM MOHAN
*Vice President & Chief Technical Officer, Afilias*

RAJESH CHHARIA
*President, Internet Service Provider Association India (ISPAI)*

# STRATEGIES FOR ATTACKING CYBERATTACKS BEFORE THEY HAPPEN

*Ram Mohan, Vice President & Chief Technical Officer, Afilias*

While Estonia was one of the first known targets of a politically motivated cyberattack in April 2007, it was not the last. There are many examples that have, unfortunately, happened since then: in 2010, there were major DDoS attacks associated with territorial disputes between China and Japan, as well as the ongoing political turmoil in Burma and Sri Lanka. In 2011, the Hong Kong Stock Exchange had to suspend trading in well-known companies such as HSBC and Cathay Pacific because their systems were under a massive DDoS attack. In 2012, the Spamhaus Project website and email systems were plagued with yet another massive DDoS attack.

I can speak from direct experience that vigilance is required in monitoring for – and protecting against – DDoS attacks. My company manages a significant portion of the domain name system and operates authoritative directories in dozens of locations around the world. We are no stranger to DDoS attacks. But this awareness of the threat, and the need to prepare against it, has yet to fully permeate governments and mainstream companies. Many times, these entities are unaware of DDoS attacks until it is too late to prevent them.

Recently, I noted during a panel presentation hosted by the Public Interest Registry and the Internet Society's New York chapter that an enormous DDoS disaster is waiting to happen. Staying ahead of potential attacks is a huge, expensive challenge on literally a global scale.

That is why I fully support the position of Toomas Hendrik Ilves in preparing against the threat of DDoS attacks rather than addressing them as they happen. Cooperation among all infrastructure providers to support the Network Working Group's Best Current Practices on defeating DDoS attacks (BCP038) is critical to the world's ongoing success in preventing future attacks. BCP038 outlines a simple, effective and straightforward method for using ingress traffic filtering to prohibit DDoS attacks that use forged IP addresses to be propagated from behind an aggregation point of an Internet Service Provider (ISP).

Building on that work is ICANN's Security and Stability Advisory Committee (SSAC), specifically the "Securing the Edge" memo (SAC004) that discusses DDoS security issues with recommendations for improvement. Of special note from this document: "From the point of view of almost any single purveyor – or consumer – of operating system and application software, convenience will almost always have more perceived value than security. It is only when viewed in the aggregate that the value of security becomes obviously higher than the value of convenience."

That is why, despite my support of Toomas Hendrik Ilves' take on preventative security against DDoS, I disagree with him in that a single unified identity is essential to online security. Ilves says: "Identity lies at the core of security online … The key to all online security is a secure online identification system."

End users' preference for ease of use is the greater issue. Users tend to take the simplest route with their technology. For example, do you enter a password each time you open your smartphone or wake your computer from a screen saver? Until you're participating in security – whether it's locking a phone when it's not in use or signing into a device with a password or fingerprint swipe – you don't fully appreciate its value until you lose your phone or someone steals important information from your computer. Then you'll be glad about the seconds you spent securing your device.

There is no better way to help governments and organizations acknowledge the importance of security than by having its members participate actively in it. Reducing that participation to a single identity, though, does not necessarily help prevent larger security issues.

I counter Ilves' thoughts in regard to a secure online identification system. I believe that idea is contrary to the fundamental privacy tenets of the Internet; an online identification system eliminates anonymous access and reduces privacy. Further, there is no evidence that the world needs a single identity scheme to prevent DDoS attacks or other Internet mischief.

A distributed denial of service attack is every organization's worst nightmare. One minute, everything is as normal. The next, the infrastructure is hit by a tsunami of spurious traffic from across the Internet. Legitimate users find themselves locked out; government and private business grinds to a halt, and there's not a great deal to be done about it.

Rather than focusing on the issues of identity, I urge all organizations to take the following steps in order to mitigate the risk of users and customers suffering disruption during a DDoS attack.

**Over-provisioning:** Many DDoS attacks are brute force in nature, and over-provisioning is a brute force defense. Your opponent simply needs to throw enough traffic at you to overwhelm your capacity. You can reduce the chances of success and limit the impact on users by provisioning for far more traffic than you would expect to receive during normal operation. Prepare for traffic many multiples of what you experience in normal operations.

**Remote/redundant monitoring:** In-house monitoring systems can be of limited utility if you are under a DDoS attack. You should subscribe to a third-party service that monitors your site around the clock, evaluating your site's responsiveness from an end-user perspective and providing alerts to your phone when problems are found.

**Dump the logs:** Your Web server logs can't tell the difference between a genuine visitor and a botnet node. Both visits will usually be recorded in the same way. While the log data could possibly be used for forensic purposes after the attack is over, its value is limited. If you find log files growing large quite quickly, you're faced with the choice between keeping the data and losing the server, or losing the data and keeping the server. If your Web server is mission critical and large log files are preventing you from recovering, your choice should be clear: dump the logs.

**Know the people at your providers:** While it is technically possible to locally configure network hardware to drop some malicious packets, ideally you'll want the unwanted traffic throttled as close to the source as possible. This means that coordination with your upstream providers is a must. It's essential to have the direct telephone numbers of contacts at your ISP's network operations center. If you know how to contact the right person to help shut down the attack, regardless of the hour, you'll experience far fewer headaches when a DDoS strikes.

# INTERNET GOVERNANCE AND CYBERSECURITY

*Rajesh Chharia, President Internet Service Provider Association India (ISPAI)*

The IGF is a platform on which we discuss multi-stakeholders, cybersecurity, openness, and access. In Hyderabad, India, we also raised the issue of the Internet for all. The open and transparent nature of the Internet means it has become all-pervasive in our lives. However, this openness has also led to certain threats, which can affect any individual, corporation, or nation.

Cybersecurity is currently the leading concern for major economies and its target can be anyone: a government department in any country or even an ordinary person. Threats have risen as the Internet has become a critical infrastructure for the global economy, with thousands of operations migrating onto it. Reports indicate that between April and December 2012, the types of threats detected on the Google Android platform increased by more than thirty times, rising from 11,000 to 350,000. They are expected to reach one million in 2013, according to security company Trend Micro.

The cyber threats and cyber attacks also reveal an escalating digital Cold War. While the United States government has claimed for years that cyber attacks are mainly state-sponsored and initiated predominantly by China, Iran, and Russia, recent reports indicate that cyber attacks in March 2013 were most frequently launched from Russia and Germany, followed by Taiwan and the United States.

That's not all. Online child abuse in the form of pornography, bullying, racism, and so on is on the rise. In the UK, 57% of 9- to 19-year-olds say they've seen online pornography, 46% say they've given out information they shouldn't have, and 33% say they've been bullied online. According to ITU surveys, 30% of teenage girls say they have been sexually harassed in a chat room; only 7% tell their parents for fear their online access will be limited. This increase clearly indicates that, as the global economy depends more and more on the Internet, the latter becomes increasingly insidious. In understanding the efficiency of the Internet, the need of the hour is to have a global effort to preserve its best aspects and guard against abuses.

Created as a decentralized network, the Internet has been a difficult place for policymakers seeking to enforce the laws of the real world. What is concerning is that in cyberspace, attacks seem to have a structural lead over defense capabilities: it can be prohibitively difficult to foresee where, how, and when attackers will strike.

Confronted with this challenge, the global community faces a dilemma between the neutrality of the Internet and cybersecurity critical services, such as e-commerce or e-health, which might never develop if users are not able to operate in a more secure environment. Moreover, some governments simply do not like ideas to circulate freely. Many governments have created national firewalls to monitor and filter the flow of information on the network. In fact, the US government, which has championed Internet freedom initiatives abroad, has been found to be cooperating with private telecoms operators on Internet surveillance, which violates user privacy. The six-year-long snooping on customer data and violation of privacy under PRISM clearly indicate the duplicity of the US on this matter. Frankly, they have lost all credibility and locus standi on their position of customers' privacy. All non-US citizens (foreign user base) can be targeted under PRISM, as reported by the media. There has been an acknowledgement that 100% security is not possible with 100% privacy and, as mentioned earlier, it is primarily for foreign users.

Such a situation makes it imperative for countries and Internet associations to take a lead in their respective

spaces and give true leadership and positions on issues related to the Internet and genuine freedom of speech on the Internet.

The question becomes more urgent every day: should the Internet remain an end-to-end, neutral environment, or should we sacrifice Internet freedom on the altar of enhanced security? The answer requires a brief explanation of how the Internet is governed and what might change.

Since its early days, the Internet has been largely unregulated by public authorities, becoming a matter for private self-regulation by engineers and experts, who for years have taken major decisions through unstructured procedures. No doubt, this has worked in the past. But as cyberspace started to expand, the stakes began to rise.

Recent ICANN rulings have exacerbated the debate over the need for more government involvement in Internet governance, either through a dedicated United Nations agency or through the International Telecommunications Union (ITU). But there are experts who fear that if a multi-stakeholder model is abandoned, the World Wide Web would cease to exist as we know it.

Last year's World Conference on International Telecommunications, held in Dubai, hosted a heated debate on the future of cyberspace. There were divergent views. The ITU looked to expand its authority over the Internet; European telecoms operators wanted to secure more revenues by changing the rules for exchanging information between networks; China, Russia, and India wanted stronger government control over the Internet; the United States and Europe stood to protect the multi-stakeholder model of ICANN; and a group of smaller countries sought to have Internet access declared a human right.

When a new treaty was finally put to vote, unsurprisingly as many as 55 countries (including the United States and many EU member states) decided not to sign. Since then, the question of how the Internet will be governed remains unresolved.

It clearly indicates that the problems that affect cyberspace cannot be resolved easily. There are three aspects that deserve international cooperation: cybersecurity, Internet governance, and freedom of expression. Solutions exist in all three domains, but should be addressed separately.

First, cybersecurity needs a global public–private partnership and countries should formally commit to fighting botnets and refraining from government-sponsored cyber attacks. The governments should set up Computer Emergency Readiness Teams that receive notification from private parties and secure network resilience either directly or through private network operators. Operators at national and global level should agree on industry-wide codes of conduct to ensure that the flow of information between operators and public authorities is fast and reliable.

Second, there is no credible alternative to the multi-stakeholder model for Internet governance. But the United States should realize that solely domestic companies should not control major Internet assets, especially as most Internet users are in Asia (China, India, etc.). More generally, ICANN should become more transparent, structured, accountable, and represent a multi-stakeholder framework if it wants to survive as a private regulator. Stakeholders in the regions where the next billion Internet users reside, such as India and Africa, should be encouraged to participate in global decision and policymaking forums.

Third, the global community should protect freedom of expression. Universal access to a robust, neutral Internet should always be preserved as a guarantee for democracy. This will be heavily resisted since it could lead to easier anonymity for criminals, but any alternative would undermine Internet freedom.

RESPONSES

# *Civil Society*

AVRI DORIA
*Non-Commercial User Constituency (NCUC), ICANN*

CARLOS AFONSO
*Instituto NUPEF, Brazil*

# FEAR FOR, AND BELIEF IN, THE INTERNET

*Avri Doria, Non-Commercial User Constituency (ICANN NCUC)*

On first reading the two contributed papers, my feelings where of fear, doubt and some uncertainty. To imagine that the Internet had become so unsafe that only governments could save it or else we would need to give it up altogether, made me shudder. To doubt that we are up to the task of finding the proper balance between institutional and decentralized power, made me despair for the future. And since the Internet is as much a belief system as it is a complex network of technology and society, the uncertainty brought on by this doubt and this fear made me wonder if it was time to just give up on the Internet as the doorway to a better future for humanity.

Reading the propositions again, I looked beyond the excellent and convincing way the articles were crafted, and started to focus on some of the building blocks in these articles.

Fortunately I found a bit of hope in questions prompted by President Ilves' thesis. Before getting to the questions, though, I want to look at the claim that "cyber can simply render the military paradigm irrelevant." Would that this were so. In a world where, as I sit writing, some governments are using chemical weapons on their own population, while others are poised to bomb those civilian populations to punish their leaders, it is hard to accept that the "military paradigm is irrelevant." We still live in a world where governments do horrible things to their people and it has nothing to do with the Internet. This does not make Internet threats irrelevant, but it puts distributed denial of service (DDOS) attacks and other property crimes in a different perspective. And while threats to the infrastructure could be catastrophic, these exist mostly in threat scenarios, at least at this point. It is certainly prudent for critical infrastructure to be hardened and protected, including from Internet threats, but to say that we have moved beyond the barbarity of real bombs and real Weapons of Mass Destruction to a greater danger from the Internet is hard to accept.

Moving to questions, why does the existence of the bad hacker[1] and the fear that is generated of the bad hacker, cause us to change our perspective of government and make us trust it. With the examples of information gathering on citizens and others by government operatives and consultants, examples that can be found in many countries – though more egregious in some than in others, how can we pretend that governments have not become Big Brother. According to the book Big Brother is here to protect the citizens. Everything the government does is for the citizen, to keep her safe from terrorists, pedophiles and to allow industry to thrive by protecting them from privacy pirates. Does the existence of an Internet threat give us cause to forget the other threats caused by government activities against the citizenry? Estonia may be a place where, at this point in time, there is a benevolent government that would not abuse the information it collects on its citizens, but what prescience can inform us that this will last and that some future government will not descend into the same sort of barbarity we see other governments perpetrating all around us. Governments make laws, some of which turn benign activities into so-called cybercrime. In some countries, for example, publishing an article on LGBT rights is a cybercrime. In other countries it is a cybercrime to publish an article critical of a leader, or

1 I tend to think of hacker as an attribute that indicates a person has deep interest in computer network systems and has the talent and perseverance to write code that can affect the Internet or some other system of interest. I tend to believe there are good hackers and bad hackers, and am always someway distressed to see how this class of person is spoken of in a pejorative way. But perhaps governments think of all hackers as bad because they represent Schneier's distributed power, a power that most governments cannot abide.

the leader's daughter. How can governments that make such laws protect the freedom of the Internet?

Are our fears of governments nebulous as indicated in the article? I have the 'fortune' of reviewing these propositions written in the pre-PRISM era during the post-PRISM era. It is possible to look at the accusations of paranoia that remain unspoken under charges of "nebulous fears" and laugh, for the paranoids have all been exonerated. All of our countries really are spying on us most of the time, whether is metadata, ubiquitous cameras, or deep packet inspection.

President Ilves's writing discusses the fact that these days it is private companies that have the information, and it is private companies that have become a threat. This may be true, but for the most part we have voluntarily given the corporations that information and we have an expectation that they will use that information prudently. We can 'vote with our feet' if they don't. And while they often fail us, we still engage in our voluntary relationship with them because they provide us with services we value and give our lives a style we want. Even when they commit the greatest harm by giving our information to governments through secret back doors, we still forgive them because it is a voluntary relationship and they are giving us something we value for our information. I was furious with Facebook and Google for their cooperation with PRISM and other assorted information gathering activities, yet I chat with my friends about it on Facebook and Google + and looked up all kinds of information about PRISM using Google and other search engines.

Is it true that "free movement of people, goods, services, capital and ideas. … can only be accomplished if identities are secure?" (Llves 2013) Do we need government identification? Even if we do need definitive identification, does the government have to track people in order for them to have verified identities? Can technology develop a method to provide secure identities in a privacy-preserving manner, as opposed to allowing this power to governments? To say that systems need to be protected does not explain the need to know everyone's identity. The activities of many governments constitute crimes against their people's human rights; the idea of governments providing someone with a secure identity that they control is the basis of many a dystopic vision. While in e-government services governments do need to control the access, the need to do so for citizen services and rights does not extend to the rest of a person's activities and interactions. We do not need to surrender to the Faustian choice: government control or "to go back to the pen, typewriter, paper and mechanical switch."

Finally I ask, do all of the increased security and surveillance techniques make us safer, or is it security theatre in the service of other goals? One of the bulwarks of the Westphalian state has always been a controlled population with a similar world view and a common set of principles. But with the Internet, all of the fruits of knowledge become available to anyone with access. And when that happens, people start questioning the control and find ways to try and alleviate their intolerable situation. Governments create laws that fabricate cybercriminals and they then have the bogeyman they can use to make us feel safer with their protection.

In terms of Schneier's piece, I think that the "nimble and distributed powers" go beyond "such as dissident groups, criminals, and hackers." I think those who create the Internet itself, it architectures, protocols and code are the main source of the distributed powers. I also believe that they are the nimble source of the solution for the current tussles with the institutional powers and part of what gives me hope that President Ilves' vision is not the only path forward.

Yes, the cloud is unsafe. But it does not need to remain unsafe. As I write these words, I am certain that there are researchers that are looking into techniques for greater safety in the cloud; for techniques that allow secure transmission and put in place cryptographic controls that can only be accessed with binary key and are not open to system administrator access. And while it is certain that every security technique may eventually be cracked, every cracked security technique will be replaced by an improved technique. Tor was safe, got attacked, and got safer.

Technology keeps progressing and those outside the institutional framework are doing much of the work. And while some countries will try to criminalize their efforts with laws against citizen use of Internet security

mechanisms, for the most part the good hackers will succeed in creating ways for users to have safer access. While it is true that using security is not always as easy as loading a music app, it gets easier for the user all the time. On Android, for example, there are many security systems that can be installed directly from the Play Store. As time goes on, it will not only be the savvy hacker who knows how to protect themselves, the savvy kids will show their parents how to turn on the newest security mechanisms.

From my perspective it comes back to technology. What made the Internet possible was technology plus a concept of distributed control. In time institutional powers caught up, they always catch up. The trick is to stay ahead of them. What will help the Internet remain the dream is the technology that is yet to come.

Both of these documents, in their own way, ignore the possibility that the people themselves can employ technology in their random and unorganized way, to escape the conundrum. It was the technology of the Internet that gave humanity one of its first views of a world where human expression was free, where anyone could communicate with anyone and where knowledge could be shared with the rest of humanity. Often, people say the solution is not technical, the solution is legislative. But history shows that the legislative solutions either fail before the wizardly of the bad hackers or become the crimes as in PRISM and related activities. In planning new technology the good hackers can look at the gaps in previous security technology and work on closing those gaps. Yes, there is a constant race between those who want to protect rights and those who want to pry those rights from them.

There is an assumption in human rights documents such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and other covenants, that the governments are responsible for protecting the peoples' rights. But over the years many instances show that governments cannot be fully trusted to protect the citizen's rights – the efforts are at best haphazard if not actually contrary to the obligation. We have also seen technology that attempts to defend our rights. While it often fails, after repeated attack, it is often improved and does provide the protection we need; at least for a while. Certainly people need to continue the work on reforming the country they find themselves subject to. But in the meantime, while working our way toward the utopian vision where all countries honor all human rights, we need to continue creating the technological tools that can give the Internet back to the people.

Taking a historical perspective, the global Internet is a very young techno-social system and is still developing according the principles that gave us the Internet in the first place. The multistakeholder model of Internet governance, not mentioned by either author, is currently being expanded to include the governments in the hope that this will give them greater capacity to create national policies consistent with the principles of human rights that have been embodied by the Internet since its beginnings. It is in this multistakeholder policy process that we will figure out how to balance the power of the creative distributed power for freedom and the repressive institutional power for safety. Between technological improvement and multistakeholder process, I find I still have hope for a global Internet.

# NETWORK SURVEILLANCE AND THE SNOWDEN WATERSHED

*Carlos Afonso, Instituto NUPEF, Brazil*

In his interesting text, Schneier uses the concept of a feudal society to compare the different leverages individuals, groups, corporations and governments have over the Internet as it evolves, and the consequences this has for political action and control. One particular leverage area has been the practice of several countries' governments, following on the steps of the United States, for decades: surveillance in the name of national security.

Suddenly, with the Snowden watershed, this has become a ubiquitous reason for concern. People and governments have seemingly just become aware that surveillance using telecommunications and Internet networks pervades our societies, and that not only the metadata of anything we (citizens and institutions of any country, anywhere) do on the Internet, but also the very content of our transactions (be it a video streaming, a voIP call, an e-commerce transaction or just a post or a visit to a social network service) are being monitored. What is more, this systematic collection of information is conducted by telecommunications operators and large Internet application providers working under contract for intelligence agencies, and with a degree of pervasiveness that makes the 2006 NSA-AT&T network wiretapping event reported by the EFF seem like a drop in the ocean.

Governments in many nations have become major users of the Internet for a variety of public services. Estonia is a good example of how governments can use the Internet to provide e-government services. However, as rulers within their geopolitical borders, governments are increasingly wielding their regulatory, legislative or plain repressive leverage to impose controls and surveillance in the name of national security.

The recent NSA revelations are being opportunistically used by governments to propose rulings allegedly to protect their people from surveillance, but, ironically, these rulings themselves often amount to nothing less than surveillance. In the wake of those revelations some high-ranking Brazilian officials are proposing that the telecommunications regulator (Anatel) literally take over the governance of the country's logical Internet infrastructure, and the agency is already issuing specific rulings accordingly. Brazilian subsidiaries of the five transnational telecommunications companies which control the main backbones in the country are even asking the government to hand over to Anatel the assignment of „.br" domain names and IP addresses. Since 2011 these government sectors, in alliance with the telecommunications oligopoly, have been striving to cancel a government ruling from 1995 (Norm number 4) which established the Internet as a value-added service beyond the purview of telecommunications laws and regulations. This would simply amount to blowing the entire historical process of building and consolidating a pluralist system of Internet governance, which is widely regarded internationally as an exceptional achievement, to oblivion. Indeed, the Brazilian Internet Steering Committee (CGI.br), if these sectors have their way, would be reduced to an advisory commission or just be disbanded by decree.

At the same time, leading economies have developed advanced worldwide parallel networks, with gateways to the Internet, to run „protected" services. As one example, estimates show that in the wake of the US military's increasing reliance on remote-controlled vehicles („drones") for running its wars on a planetary scale, about 40 countries are doing the same, and these systems run in protected networks also using the same data connection and transport technologies as the Internet's. Similar parallel networks are deployed for a variety of wiretapping functions.

As Professor Milton Müller stated in a 2012 article, „[t]he biggest threats to Internet freedom today do not come from intergovernmental organizations. They come from national governments with the institutional mechanisms to regulate, restrict, surveil, censor and license Internet suppliers and users." [1]

In the same article Müller also states that „it was the Internet - the ability to network computers across borders, free from nation-state controls and permissions - that opened up this new world [of global communications] for us." Yes, the Internet opened up a new world of communication and integration, but it did not penetrate geopolitical borders without having to overcome diverse governmental hurdles. In several countries significant pro-Internet lobbying and advocacy was necessary to circumvent legal and regulatory barriers. This often involved confronting state telecommunications monopolies, whose anti-Internet policies included imposing absurd taxes on users' or networking equipment or preventing the new network from being established at all, even for academic purposes. In Brazil the very TCP/IP protocol was illegal (by rule the state telecommunications monopoly allowed only for OSI/ISO standards) and remained formally so until the privatization process in the late 90's, although the first permanent international links to the Internet started to operate under the protection of a host country agreement with the UN for the UNCED 92 conference.

There is one aspect of the impressive achievements described by Mr Ilves regarding the development of the Internet in Estonia, which remains elusive: Since his country joined NATO even before becoming a member of the European Union, and is a member of the OSCE, it would be interesting to know how it reconciles its exceptional cybersecurity and e-governance infrastructure with the protection of its own people against the pervasive invasion of privacy practiced by government agencies, in particular the National Security Agency of the United States.

1 www.sfgate.com/opinion/article/Greatest-threat-to-Internet-governments-3723621.php#page-1

RESPONSES

# *Technical and Academic Community*

ALEXANDER KLIMBURG
*Fellow and Senior Adviser at the Austrian Institute for International Affairs*

LEONID TODOROV
*Deputy Director, Coordination Center for .ru*

XU PEIXI
*Associate Professor, Communication University of China*

# WATERING THE GRASS ROOTS

*Alexander Klimburg, Fellow and Senior Adviser at the Austrian Institute for International Affairs*

The concept of "Internet Feudalism", as elucidated by Bruce Schneier in *Power in the Age of the Feudal Internet,* paints a stark picture of power in cyberspace. In his opinion, the struggle between "institutional power" (government and corporations) and "distributed power" (fringe groups such as activists, criminals, and hackers) is increasingly being won by the former. A "dangerous world" is increasingly leading to the creation of computational fiefs maintained by institutional powers, who themselves fight over the "peasants" (the common users) whom they exploit in return for the promise of a semblance of security. In between the fiefs, in the forest of the unregulated, lurk the "distributed powers" – likened to Robin Hoods – whose fieldcraft allows them to maintain some level of freedom from the hegemons.

This fascinating thought experiment is certainly fertile ground for all types of further historical analogies: if, for instance, common users are akin to peasants, is personal data then similar to corvée or "statute labor" (besides the obvious equivalent of "taxation" with "license fees")? Would the vaunted mercenary groups that played such an important role in European warfare in pre-Westphalian times have their equivalent in large cyber-crime gangs and hacker collectives? And, as a logical and practical consequence, would it be reasonable to assume that pursuant to Article 1 Section 8 of the US Constitution, the US government can (and should) issue letters of marque to empower cyber-"privateers" to attack enemies of the United States?

This last example was not an attempt at flippancy – in the last decade, some members of US Congress repeatedly explored options of using this somewhat antiquated provision in a number of different settings. It is certainly useful to look at historical examples to explore the current macro-picture, but more important than Schneier's historical analogies is a simple assertion: governments, as a rule, are coming to dominate cyberspace, and the "distributed powers" will suffer as a result. I would disagree that the situation is quite as dire or as irreversible as Schneier implies. Or, it is not that dire yet. For some of the institutional powers are perfectly happy with distributed power – at least in theory.

I would argue that, while it is true that "institutional power" – especially government – is (re)asserting itself in cyberspace, this does not mean that "distributed power" – which for me most importantly includes civil society – must be defeated as a direct consequence. In fact, liberal democracies – as opposed to authoritarian regimes – are, at least in theory, committed to a plurality of power structures. This does not only mean the separation of the three powers of government, or between church and state, but rather that liberal democracies as their essential *raison d'être* accept that the non-state sector must be strong and healthy for democracy to be said to truly exist.

That is a positive thing, for as Joseph Nye has pointed out In the Future of Power, the macro trend of the "diffusion of power" away from traditional forms of government power towards non-state actors could actually strengthen, and not weaken, open societies and their governments. The very rise of the Internet itself is an example of this, as the US government has continually loosened its control over the Internet Corporation for Assigned Names and Numbers (ICANN) as part of an overall belief that the Internet should not be a creature of governments. Nearly all liberal democracies have come to support this view and, in increasingly bloody diplomatic battles with authoritarian regimes fighting for "cyber sovereignty" (one of which I describe in *The Internet Yalta*), are supporting the role of the non-state sector within the multistakeholder model of Internet governance.

At least, that is, in theory. In practice, civil society is very much being pushed to the margins, as Schneier says, by the government – even by those advocating civil society engagement. Mostly, the problem is one of scale – civil society is being "outworked" by a much better resourced stakeholder group. But the situation is not hopeless. Liberal democracies are, after all, apparently convinced of the need to support civil society – although at the moment, that support has been largely verbal. Practical support, however, is urgently needed.

Civil society is facing three resource crunches that, taken together, pose a serious threat to the multistakeholder model as a whole – which depends on the equal participation of government, the private sector and civil society to make Internet governance work in the way it does today. Government and the private sector are slowly but surely (and sometimes unconsciously) crowding out civil society (i.e. academics, technical volunteers, and policy advocates) by constantly raising the bar for participation. The first challenge is the greatly increasing travel requirements for those wishing to be involved in Internet governance. The logarithmic explosion of physical meetings and conferences in highly dispersed locations is a significant resource challenge for civil society – creating a system better suited to professional diplomats rather than academics or volunteer engineers is certainly not conducive towards "equal participation". A second significant challenge for civil society is the increasing knowledge demands that are being placed on participants. The discourse is constantly widening, with those civil society experts who were previously only concerned with IETF (Internet Engineering Task Force) or ICANN documents now expected to be knowledgeable on a number of diplomatic, international security, and privacy issues – plus an expanding galaxy of technical aspects as different as GUCCI to malware reversal. For many policy and engineering specialists, it can be very difficult to break out of their respective "bubble" and to inform themselves about the main issues within related fields. Time – which often, but not always, translates into money – is usually the greatest resource barrier. Finally, security (in particular that unloved amalgam called "international cybersecurity") has gone from being a fringe topic to probably one of the most important themes within the present discourse – governments often claim security issues as being one of the main sources of their legitimacy when discussing Internet governance. International cybersecurity discussions draw much of their thematic input from classified sources. Access to esoteric information (both confidential and/or simply obscure) is increasingly becoming a valued currency within agenda-setting circles.

These three resource issues are slowly but surely eroding the role of civil society within the multistakeholder model. While liberal democratic governments have stridently backed the multistakeholder model as described in the 2005 Tunis Agenda (a UN document), they have been caught in a paradox of their own making: the more governments talk about the importance of civil society, the more they are tacitly diminishing it.

But what are the options? Obviously to cease discussions about civil society would be even worse than the present "talking over" (rather than with) it. The only other option would be to diminish the amount of frantic activity so that civil society has a chance to "catch up" – if anything, even more unlikely. That leaves only one option: materially supporting civil society directly. In a phrase: watering the grass roots.

How can this be accomplished? The first and most obvious need is tangible – increased funding is desperately required. Additional funding could help scholars devote more time to the rapidly expanding scope of Internet governance, rather than chasing grants in unrelated fields to help pay the bills. Civil society organizations could hire more staff and expand their level of engagement. Various technical/educational programs could be provided for those volunteers wishing to broaden their skills. And everyone could use additional travel money.

Where should the funding come from? In the United States, civil society is largely synonymous with philanthropy – from foundations, corporations and, increasingly, wealthy individuals. The government does play a role, but largely as the provider of research grants – not as an institutional backer, even if the difference is rather one of semantics, given the role of federal research grants. Outside the US, the role of the state in supporting civil society is widely practiced. Besides the considerable sums spent financing tertiary education in all its forms, many think-tanks and even advocacy

groups receive government subventions. Sometimes this has led to US bodies sneeringly categorizing such groups as GRINGOs (Government-regulated NGOs), although their independence can be even more robust than a think-tank completely at the whim of a single benefactor. There is, in fact, little evidence to support the contention that government subventions come with more strings attached than support from the private sector. Indeed, even a cursory examination of this situation reveals the exact opposite.

One of the most interesting financing models in the area of Internet governance does not involve conventional philanthropy at all. The Internet Society (ISOC) finances itself largely through the sale of .org domains, and there is no reason that in the new generic Top Level Domain (gTLDs) world (such as .newspaper or .computer) similar arrangements couldn't be possible. For instance, it may be interesting to revisit the ban on ".country" gTLDs (such as ".mexico" or ".germany"), as long as the proceeds are earmarked to support civil society engagement. Having said that, ICANN has already accumulated at least USD 130 million in order to protect itself against possible litigation over the new gTLDs – maybe some of that cash could be put to more immediate use.

Government can help address a second resource barrier for civil society, namely a limited understanding of "international cybersecurity" issues. This term is a catch-all concept that includes a wide range of topics – from debating the applicability of international law to the organization of specific national cybersecurity bodies and the use of various technical tools in intelligence and cyber-attack. International cybersecurity is rapidly becoming an important narrative for governments engaged in Internet governance. To this day, however, much of civil society has tried to resolutely ignore security issues – ICANN has recently even inexplicably decreased the role of its security team. This is a major mistake – there are serious security issues related to cyberspace, and, equally importantly, governments derive much of their legitimacy from national security concerns related to cyberspace. Obviously most of the actual cybersecurity work is undertaken by non-state actors rather than government. However, government has a useful role to play as a point of interlocution in this often nebulous world with its very multifaceted, and often seemingly esoteric, concerns.

Government support could even extend to offering members of civil society classified briefings on incidents, and with the corresponding security clearance. This could prove particularly valuable in instances where civil society has an assigned arbitration or advocacy function. For instance, one of the proposals related to the reform of the US Foreign Intelligence and Surveillance Court (FISC) foresees a "special privacy advocate" – coming from civil society – who would challenge the NSA on specific collection efforts. One issue is, however, that for some countries (especially the United States) only the highest clearances would be useful, and those often come with a level of scrutiny that few civil society actors are willing to tolerate.

Another way for civil society actors to get a feel for international cybersecurity concerns is to become directly involved in multilateral or bilateral government cybersecurity discussions. Here, in contrast to the Internet governance context, the state clearly dominates. This often leads to one-sided debates when discussing "confidence building measures" or "norms of state behavior" – where the fundamental role of civil society bodies such as the IETF or others is often blissfully ignored by governments. It is not strictly speaking necessary for civil society actors to actually be present at these discussions – just being aware that they are occurring, and formulating and presenting position papers to the agencies responsible, could provide a much needed diversity of perceptions and solutions. This would, however, require proactive engagement on behalf of civil society to redress this entrenched imbalance, as very few civil servants actually actively reach out to civil society in the context of those discussions.

The lack of government outreach was recently expressed by a seasoned official in the context of the 2012 WCIT conference in Dubai: "I want to support civil society – not talk to them. That's always a waste of time[1]." Effectively, many civil servants have decided that while they will fight to the death to "defend" the right of civil

1 ascribed to Alexis de Tocqueville presenting on "Democracy in America" (1835).

society to engage in the multistakeholder model, at the same time they really do not want to listen to them. They value civil society as a symbol of democratic freedoms, but not as an entity that is actually practical or particularly useful. This is largely incorrect, and in any case beside the point. Besides the obviously vital function that parts of civil society have played in the rise of the Internet, their undoubted practical contributions are outmatched by their overall importance for democracies as a whole. Perhaps the greatest difference between the world's authoritarian regimes and true liberal democracies is the healthy functioning of civil society – this may even be the only real "unique service proposition" of freedom. As Alexis de Tocqueville once said: "The health of a democratic society may be measured by the quality of functions performed by private citizens." [2] Perhaps the same holds true for the Internet.

2 Private communication.

# CYBERSECURITY AS AN INSTITUTIONAL CHALLENGE

*Leonid Todorov, Deputy Director, Coordination Center for .ru*

I was amused to see Messrs. Ilves and Schneier's papers offer provocative insights and encourage a closer look into the problem of a cybersecurity institutional framework. They force one to ask three questions: (1) Why does the State perceive cybersecurity to be such a plumbing issue these days? (2) Should cybersecurity fall under the State's exclusive mandate? (3) What are we, as a community, expected to do?

The first question suggests employing the institutional theory perspective, and individuals' rational and opportunist behavior and the State–individual relationship in particular.

The substance of the relationship appears fairly elusive and can easily be abused and manipulated by an individual or a certain group, including, for example, an attempt to spook other individuals, thereby forcing them to accept whatever the State believes (or seems to believe) in.

It is common knowledge that human beings have a natural propensity to exaggerate certain dangers. In the case of organized crime, for instance, do we seriously believe the Mafia are waiting for us around each and every corner? This is absurd, of course, caused by our limited rationality – even the mob's violence-related capacity is limited and they have to save precious resources.

So much about cybersecurity. While hardly a manipulator, Mr. Ilves's assumption about "ruining a country by bringing its Scada system to a halt" and the call "to re-examine many assumptions of security" and for "rethinking some of our core philosophical notions of modern society [in particular] between the public and private spheres" are a very familiar mantra, easy to sell to the public at large, yet only partially true at best and a pretty good example of a statesman's biased rationality. Indeed, political scientists, economists, etc., and even governments themselves have long shared a misconception about the State as an omnipotent, uber-benevolent and superintelligent subject, which would take one's great idea and efficiently and promptly implement it for everyone's benefit. This sense has become particularly predominant since the 2008 crisis [1]. The problem, however, is that the State is not transfinitely rational, as its rationality effectively constitutes a sum of the rationalities of the individuals in power. So, a bet on the State's omnipotence rests upon an utterly unrealistic idea that we are ruled by Olympians. The State does not appear too benevolent either, as opportunistic behavior is possible both beyond the circle of power and within it. Factor in effects from a negative selection of public servants and we may well end up facing an immoral bunch in power, keen to manipulate and mislead us for their own purposes. Quite illustratively, Pres. Ilves ascertains, "If the private sector is unwilling to take the necessary steps to guarantee the integrity of its online activities [Is it? – L.T.], the government must step in [Must it? – L.T.] to fulfill its most fundamental task – to ensure the security of its citizens … [Is that the prime task indeed? – L.T.]". Small wonder that he then shoots forth a pretty hip Orwellian oxymoron that "The job of **cybersecurity** is to enable a globalized economy based on the **free** movement of people, goods, services, capital and ideas" – all under Big Brother's gentle but close observation, needless to say.

Do we really like living in this brave new world? Laying hopes on something supermighty and uber-benevolent is unlikely to form a normal bearing. Rather, we – or as Bruce Schneier puts it "everyone in the middle" – should

1 With big banks and corporations kowtowing and begging for bailouts, even a most rational State would feel like a real savior, with ultimate wisdom and powers to decide everyone's fate.

also be keen to rely on specific, non-rigid institutions in the form of rules of social interaction, commonly agreed upon (between us), as much as common sense.

Back to institutional theory, the phenomenon we now know as James Buchanan's goods implies a "normal" good on sale in tandem with certain contractual packaging, rules and institutions: thus, the choice between different goods, as well as different institutions, is ours. It's therefore a blessing that, stuck between the power of big corporations and nation states, we are watching "Game of Thrones … when powers fight: when Facebook, Google, Apple, and Amazon fight it out in the market; when the US, EU, China, and Russia fight it out in geopolitics … ", for their unlikely global alliance would otherwise put an end to our ability to make a rational choice about fundamental matters, including cybersecurity.

Rational choice should be guided by the conscious realization that cybersecurity does not form the State's exclusive mandate – it is to a great extent an individual's personal matter too. Once again, many things we have allowed the State to misguide us with are in fact phantoms from the abyss of our underconsciousness and we often do not need the State to play the role to the extent it forces us to believe is imperative [2]. And I fully subscribe to Bruce Schneier's call "to decide on the proper balance between institutional and decentralized power, and how to build tools that enable what is good in each while blocking the bad" and Mr. Ilves's essentially similar observation that "Cybersecurity is not just a matter of blocking bad things … it is protecting all the good things that cyberinsecurity can prevent us from doing".

We now have three intertwined institutional vehicles, that is: enhanced cooperation, the IGF, and multi-stakeholderism. While of different origin, they pursue the same objective and, combined, form a powerful instrument to promote debate on the future of the Internet and its governance system. Promoting the use of the vehicles and drawing the maximum from them is our prime mission as a community.

I fully share Mr. Schneier's uncertainty about the path of future developments; however, with the State having compromised its credibility with all sorts of online eavesdropping initiatives, a drift towards "secure islands" seems inevitable. That said, security there may not necessarily be run by a "Sheriff of Nottingham" or a corporate executive, for it may well be a genuine netizen community that designs and enforces institutions of its own, which I would not mind at all. Would you?

2 In this context, it is worth revisiting R. H. Coase's famous paper "The Lighthouse in Economics" (Journal of Law and Economics, 1974, 17 (2)) a truly eye-opening illustration of how misguided we may be in regard to the actual role of the State in (economic) development.

# DEFENDING COMMON SENSE IN THE 2013 CYBERSECURITY DEBATE

*Xu Peixi, Associate Professor, Communication University of China*

To comment on a timely article by Bruce Schneier, I shall attempt to deliver a few observations deriving mainly from the 2013 cybersecurity debate between China and the U.S. If I can succeed in asking the right question about this China–U.S. row, it would only make his thesis more convincing by complementing it with a fresh case study, but if I fail to do so, I ask to be forgiven for running against some of his judgments. Among all the merits, Schneier's conceptions – such as the quick vs. the strong, or "nimble distributed power" vs. "ponderous institutional power", or metaphorically put, "Robin Hood" vs. "the Sheriff of Nottingham" – hold the key to many myths about the degree to which we are empowered by the Internet. He presents valuable concepts such as the "security gap", defined as a "time period where the nimble distributed power can make use of new technologies before the slow institutional power can make better use of those technologies".

With the help of these concepts, we can distinguish between the early days of the Internet, when the citizens were winning, and what is happening right now, when governments and corporations are gaining the upper hand. Schneier's text captures this exact dimension of momentum: the development of the Internet is about to repeat that of radio and TV, which was once characterized by a similar early period of optimism. The fight over broadcasting was over and political and commercial forces declared victory; however, the battles over the Internet are ongoing and we still have a slim chance of winning. The last paragraph of Mr. Schneier's text lists a few mechanisms –legislatures, ITU, IGF – through which we need to engage in these debates to "to build tools that amplify what is good in each while suppressing the bad".

As a civil society stakeholder from a developing country, I want to deliver my observation here in particular on how the bigger and stronger institutional powers represented by the U.S. and Google divert the attention of the global public by inventing, fabricating, or exaggerating the cybersecurity threats from other countries while the fact is that they are threatening, hacking, and harassing others. These games add much complicity to the Internet governance debate at global forums. And they have so far scored tremendous success in preventing the formation of a global solidarity among the global public. What should be a common cause against all institutional powers, both in the global North and global South, is skillfully framed by these super powers as a fight within their same species of institutional powers. Those powers like the U.S./Google – that is, themselves – are associated with positive words such as freedom, free flow, and innovation. Those powers like Iran/Russia/China/Saudi Arab/Africa/Huawei are often associated with negative words such as censorship, control, surveillance, and theft.

Before a young Edward Snowden spoke up, Google accused the Chinese government of accessing "the accounts of dozens of U.S., China, and Europe-based Gmail users". The U.S. government accused the Chinese government of hacking into U.S. computer systems and stealing intellectual property from numerous American businesses. American politicians, from the bottom to the very top levels, were collectively engaged in a China-bashing campaign. A record number of American institutions, from the Justice Department to Congress and the Pentagon, spoke with one voice that was ruthlessly recycled by the commercial media. A powerful hurricane of curse and condemnation took shape and force. The topic had been pushed to such extremes that some were discussing the imminent danger of state-sponsored Chinese hackers attacking American infrastructures, including telecommunications, power grids, airports, and nuclear facilities.

Mr. Edward Snowden then exposed the comprehensive espionage activities the U.S. had been conducting against China and other countries, with the willing and full cooperation from its information industry. American accusation fell flat on its face and the gigantic hammer highly lifted dropped on its own foot. To paraphrase Warren Buffett, when the tide goes out, you get to see who's swimming naked. In the wake of this, I ask two questions. What do we do when the U.S. and Google, who monopolize the core Internet resources and are located on the upper side of the river, are acting foul and doing evil (or at least acting inconsistently)? The question becomes more acute when the topic of cybersecurity is linked with national security and is being justified as a rationale to start physical wars. Then, naturally, we ask: to what degree is the concept of national sovereignty of the Westphalian System valuable or outdated?

The answers to these questions are hard to give, but the way we answer the questions with actions will bring us three scenarios for the future Internet. **Scenario 1** is that the bigger institutional powers find it suitable and profitable to succeed in repackaging and selling a Cold War mentality to the public in the global North. In this case, national sovereignty would remain the best rationale for the global South to defend their interests inside and outside cyberspace and will hold its value in the global Internet governance forums. **Scenario 2** is that the smaller, weaker institutional powers are forced or bribed to operate as the agents of globally more dominant ones. That is what is happening now. You may observe that the cybersecurity row between China and the U.S. was quickly brushed aside during the 5th China–U.S. Strategic and Economic Dialogue when the Chinese side agreed on a number of frameworks for a future investment treaty, which would mean more economic penetration of the Chinese market by American businesses, but Chinese businesses in the American market can be resisted using the rationale of national security. The China–U.S. relationship can be as good as a couple (China–America) or as bad as an enemy (anybody but China), depending on American business interests. The EU, if we categorize it as an institutional power, will remain dominated by the British position as a close ally of the U.S. and shy away from its initial public model of Internet governance, which should have succeeded now as a political compromise. This scenario would mean more solidarity of the institutional powers and more marginalization of the global public, and it is more likely to happen. **Scenario 3** is what we are working for. That is, we, the distributed and fragmented powers with fewer resources but more moral legitimacy, will not stand by and watch the miraculously played out good cop vs. bad cop show presented by the institutional powers. We will take action to tame both the global and local feudal lords.

# AUTHORS

**Carlos A. Afonso** is currently executive director of the Nupef Institute and chair of the Brazilian chapter of ISOC. He has been a consultant on themes related to ICTs and human development for several countries and international organizations. Afonso is a.o. co-founder of APC. He holds a Master in Economics, York University, Toronto, Canada, with doctoral studies in Political Thought at the same university.

**Dr. Olga Cavalli** is an electrical and electronics engineer. She is currently the President of the Women in Technology and Business Forum as well as, among others, Argentina's GAC representative at ICANN, Latin American Director at South School on Internet Goverance, professor at EURO-SSIG and adviser for technology at the Ministry of Foreign Affairs.

**Rajesh Chharia** is a Member of the Delhi ISOC Chapter at Internet Society, President at Internet Service Providers Association India (ISPAI), Director at National Internet Exchange of India (NIXI) Ltd, Owner & CEO at Chandra Indl Co Pvt Ltd and CEO & Promoter at CJ Online Private Limited.

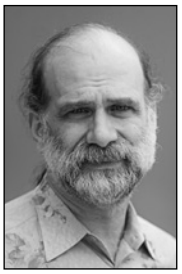
**Avri Doria** is a technologist involved in the development of Internet protocols and architectures. She is a.o. participant in the IETF, Chair of the IRTF Routing Research group, Technical Committee Chair of the Multi Service Forum, a member of the ICANN GNSO council and was a member of the WGIG. Doria is co-founder of the Nomadic Women's ICT Network and member of the APC Women's Networking Support Program.

**Toomas Hendrik Ilves** is President of the Republic of Estonia. Ilves served a.o. as the Ambassador in Washington and as Minister of Foreign Affairs. He is currently Chairman of the European Cloud Partnership Steering Board and has written extensively on European integration, transatlantic relations, e-government and cyber security. Ilves holds a Master's degree in Psychology from the University of Pennsylvania.

**Thorbjørn Jagland** is Secretary General of the Council of Europe and Chairman of the Nobel Committee. He was previously President of the Norwegian Parliament, Prime Minister and Minister of Foreign Affairs. Jagland is the Chairman of the Board of Directors at the Oslo centre for Peace and Human Rights. He holds a degree in Economics from the University of Oslo and has published widely on international affairs.

**Alexander Klimburg** is a Fellow at the Austrian Institute for International Affairs. Klimburg has undertaken government national security projects for a.o. the Austrian Federal Chancellery, the Ministry of Defense, and the National Security Council. He has partaken in international and intergovernmental discussions, and acts as an advisor to the Austrian delegation to the OSCE as well as other different bodies.

**Ram Mohan** is Executive Vice President & CTO of Afilias Ltd. He is one ICANN's Directors and founding member of SSAC. Mohan serves on the steering committee of APWG and the Advisory Committee of ISOC. He is advisor on Internet security and globalization issues and the creator of the technology behind TurnTide. He has a Bachelor's degree in Electrical Engineering and an MBA in Entrepreneurial Management.



**Bruce Schneier** is a renowned security technologist He is the author of best-sellers like Applied Cryptography, Secrets and Lies, Beyond Fear or Schneier on Security. Schneier also publishes Crypto-Gram, a monthly newsletter and one of the most widely read forums about security. He holds an MS degree in Computer Science from American University and a BS degree in Physics from the University of Rochester.

**Leonid Todorov** holds a M.A. in Linguistics from Moscow State Pedagogical University. He serves as Deputy Director for External Relations in Russia's Internet registry. Todorov has written extensively on Internet governance, new gTLDs and cybersecurity. He is on the Steering group of EuroDIG, the CCNSO ICANN's Strategic and Operations Plan Working Group, and on the ISOC Advisory Council.

**Xu Peixi** is Associate Professor at Communication University of China, Beijing. He is also PhD candidate and researcher at the University of Tampere, Finland. His research interests include international communication, citizen participation, media and local administration and new media.

# ABOUT THE COLLABORATORY

The **Internet & Society Collaboratory** is an internet policy think tank and discourse platform based in Berlin. Its mission is to analyze developments in the context of the digitisation of our society from diverse angles with relevant stakeholders and to come up with ideas and solutions. Our multi-stakeholder approach guarantees transparency and independence. The experts' transdisciplinarity allows for the transformation processes to be apprehended in their entire scope. We identify possibilities and risks and discuss their implementation in direct dialogue with decision makers.

For this purpose, the Collaboratory brings together experts from civil society, the private sector and academia, in order to contribute their expertise via **initiatives, open working groups** and publications. The initiatives bring together around thirty people and span several months, focussing on a major aspect, currently e.g. "Globalization". The collaborative work of the expert groups leads up to a final report, containing recommendations or describing scenarios. Working groups are long term project incubators, conducting studies, organizing conferences and picking up on early trends in internet policy.

Conceived as a Community of Practice, the Collaboratory is open to contributions from the most diverse angles regarding its form, its processes and its results and is continuously developing as a "perpetual beta". The Collaboratory is open to new experts and partners.

The Internet & Society Collaboratory was initiated by Google Germany in 2010. Today, Wikimedia Germany, Creative Commons, Fraunhofer FOKUS, the W3C office Germany-Austria, the SMBS, the German Chapter of the Open Knowledge Foundation, the DFKI and CSC Germany are among our ooperation partners. Since August 2012 it is a registered non-profit based in Berlin. Contact us today to join us as a supporting partner!

# PREVIOUS ISSUES AND AUTHORS OF MIND


**MIND 1**
Grundrecht Internetfreiheit


**MIND 2**
Internet Policy Making


**MIND 3**
Grenzen der Internetfreiheit


**MIND 4**
Human Rights and Internet Governance


**MIND 5**
Internet und Demokratie

Alphabetic list of authors of the discussion paper series (the spring issue is in German, the fall issue in English). If you are interested in joining the debate, please email the editor. Find all previous publications in electronic formats on en.collaboratory.de/w/MIND

## A

Fiona M. Alexander

## B

Christian Bahls
Wolfgang Benedek
Carl Bildt
Jermyn Brooks

## C

Vinton G. Cerf
Olivier M. J. Crépin-Leblond

## D

Hans Peter Dittler
Bertrand de la Chapelle
William J. Drake

## E

Shirin Ebadi
Raúl Echeberría
Anriette Esterhuysen

## F

Alvar C. H. Freude

**G**

Philipp Grabensee

**H**

Cees J. Hamelink
Bernd Holznagel
Sandra Hoferichter
Peter H. Hellmonds

**J**

Thomas Jarzombek
Zahid Jamil

**K**

Matthias C. Kettemann
Markus Kummer
Dirk Krischenowski
Angela Kolb
Andreas Krisch
Ronald Koven
Wolfgang Kleinwächter

**L**

Sabine Leutheuser-Schnarrenberger
Wolf Ludwig
Everton Lucero
Joy Liddicoat

**M**

Erika Mann
Annette Mühlberg
Sivasubramanian Muthusamy
Tobias Mahler
Alice Munyua
Jeremy Malcom

**N**

Julian Nida-Rümelin

**O**

Wolf Osthaus

**P**

Ingolf Pernice

**R**

Michael Rotert
Kenneth Roth

**S**

Marietje Schaake
Klaus Stoll
Pascal Schumacher
Erich Schweighoefer
Nicolas Seidler
Jimmy Schulz
Christian Stöcker
Christoph Steck
Oliver Süme
Graciela Selaimen
Waudo Siganga
Theresa Swineheart
Irin Shebadi
Thomas Schneider

**T**

Matthias Traimer
Catherine Trautmann

**V**

Sabine Verheyen

**W**

Karola Wille
Rolf H. Weber

# IMPRINT

***The Collaboratory Discussion Papers are a publication by the Internet & Society Collaboratory***

***Editor***
Wolfgang Kleinwächter

***Production***
Sebastian Haselbeck (co-editor) – Lorena Jaume-Palasí – Gordon Süß

***Layout & Design:***
Jan Illmann

Original design concept of the series
Jessica Louis & Sabine Grosser
www.louisgrosser.com

***Printed by***
Best Printing (Bali)
Oktoberdruck (Berlin)

***Contact the Collaboratory or its board***
Dr. Philipp S. Müller, Dr. des. Ulrike Höppner, Martin G. Löhe,
Dr. Marianne Wulff, John H. Weitzmann
kontakt@collaboratory.de

Visit us at www.collaboratory.de




"Internet and Security". MIND Multistakeholder Internet Dialog #6. Collaboratory Discussion Paper Series No.1, Internet & Society Collaboratory www.collaboratory.de – Berlin & Bali: October 2013

Internet & Society
Co:llaboratory

The Internet & Society Collaboratory is an open think tank and internet policy deliberation platform dedicated to enabling the interdisciplinary work of specialists from civil society, academia, the public and private sectors on solutions to tomorrow's socio-political opportunities and challenges posed by the digital progress at the interaction between the internet and society.

Please contact us via international@collaboratory.de if you require more information or if you are interested in participating in our projects.

The Collaboratory is a registered non-profit organization based in Berlin. It was originally initiated by Google Germany. For more information on the Collaboratory, our projects and activities, our funding and participating experts please visit collaboratory.de

*Visit the Internet & Society* Collaboratory *at:* ***http://en.collaboratory.de***



ISBN 978-3-00-043691-8