TRAVEL GUIDE TO THE DIGITAL WORLD:
CYBERSECURITY POLICY FOR HUMAN RIGHTS DEFENDERS

Carly Nyst

Published in London 2016
by Global Partners Digital

“It sounded like it meant something or it might mean something, but as I stared at it, my whole delight was that I knew it meant absolutely nothing”.

William Gibson, recalling his invention of the word ‘cyberspace’

In the last few years, you may have noticed the increased prominence of a certain prefix.

Lurid stories of 'cybercrime' and 'cybercriminals' abound in the media. 'Cyberbullying' and 'cyber harassment' are widely acknowledged social problems. In anticipation of 'cyberthreats' or 'cyberterrorism', states conduct 'cyber exercises' and sign high-profile 'cyberpacts' or 'cyberagreements' with other states. A rapidly expanding domain of 'cyberlaw' tries to keep pace with it all.

The curious thing about 'cyber' is that the more it is used, the less meaning it seems to hold. Cyber can encapsulate everything and nothing at the same time. To locate the reasons for this elasticity, a brief look at the word's history might be helpful.

The story begins with the Ancient Greek word 'kubernesis', meaning steering, control or governance. Several thousand years later in 1940, an American mathematician, Norbert Wiener coined the word 'cybernetics' to describe the emerging field of robotics.

In 1982, a significant mutation occurs. In a short story, science fiction writer William Gibson invented a new word, 'cyberspace', to describe an abstract and ungovernable realm. Here, crucially, the connotation is with anarchy - not control. The word quickly became synonymous with the emerging digital environment; its prefix a means of bringing offline phenomena into an online context.

Today, cyber has in some respects come full circle. The ungovernable space evoked by Gibson has disappeared. Cyberspace is now indisputably a zone of contention for states, subject to increasing control and governance; and new words like cyberwar, cybercrime and cybersecurity all carry with them the notion of categorising and governing the mass of actors, spaces and practices that exist in the digital universe.

Amid all this, it is the word 'cybersecurity' which has become most dominant. It is an objective tirelessly invoked and pursued by governments through policy. It is used to refer to anything from digital literacy programmes, to laws with sweeping new surveillance powers.

But what, exactly, *is* cybersecurity - and why should cybersecurity policymaking matter to human rights defenders?

AN OVERVIEW OF THIS GUIDE

Human rights defenders play a critical role in ensuring that government policy adheres to established human rights norms. When human rights defenders are absent from policymaking, there is a risk that important policy decisions will be driven by short-term political gain, rather than the promotion and protection of human rights. The capacity of human rights defenders to input into and scrutinise public policy depends on their having a base level of knowledge of the relevant institutions, stakeholders and issues at stake.

When it comes to cybersecurity, it is increasingly evident that human rights defenders do not, on the whole, have this capacity. In fact, there is not even a shared understanding of what cybersecurity is. Depending on who you talk to, and in what forum, cybersecurity can extend to issues as diverse as security protocols in government databases and the international norms applicable to **cyber-attacks** during armed conflicts.

At a fundamental level, human rights defenders are also impeded by the lack of an agreed language with which to discuss cybersecurity. Many of the concepts in this domain – such as 'cyber-attack,' 'information security', and 'cyber conflict' – have contested meanings, which are subject to ongoing debate, and – in some cases – manipulation for political ends.

This guide aims to help correct the imbalance in capacity and expertise between human rights defenders and cybersecurity professionals and policy-makers.

At the heart of the guide is an attempt to address perhaps the fundamental barrier: the absence of clear definitions and agreed terms. It will do this by closely examining three separate policy areas which are often conflated under the umbrella of cybersecurity – information security, cybercrime, and cyber conflict – unpacking their policy and legal dimensions, mapping relevant stakeholders, and outlining the issues at stake. It is hoped this will help human rights defenders engage effectively in cyber policy debates at the domestic, regional and international levels.

Chapter 1 covers the basics on cybersecurity: what it is, its relationship to human rights, and where the policies are coming from. Chapter 2 explores the human rights implications of a range of information security issues, including the need for international technical standards on cybersecurity and information-sharing on cyber threats. Chapter 3 puts cybercrime legislation in the spotlight, looking at what it regulates and the types of measures it incentivises, including **mass surveillance**, bans on **encryption** and steps to undermine online **anonymity**. In Chapter 4, the guide moves to cyber conflict and the evolving debate on the application of international relations norms to cyberspace. In each section, we suggest ways human rights defenders can bring human rights into cybersecurity policy debates – and at the end we propose some general principles for human rights engagement with cybersecurity policymaking. This guide is aimed at a non-technical audience, so we have also added a Glossary at the end where words in bold print are explained.

This guide comes with a caveat. Cybersecurity is a rapidly growing and changing area of law and policy. There remains little consensus, especially amongst governments, about the scope and application of cybersecurity – let alone its relationship to human rights. The views expressed here are therefore those of one actor amongst many, and the categorisation of issues adopted here is neither exhaustive nor definitive.

In this emerging domain, human rights defenders will need to do more than just policymaking. They will need to be active in shaping the very definition and remit of cybersecurity policy – what it covers, what it means, what it includes and excludes. If this task is left to security professionals and governments alone, the likelihood of policies emerging which strengthen individual security and uphold human rights does not seem high.

CONTENTS

CHAPTER 1

UNDERSTANDING CYBERSECURITY

Understanding Cybersecurity

Cybersecurity is an unstable and contested term, encompassing a range of possible meanings. Understanding what these are is a crucial first step to effective engagement.

DEFINING CYBERSECURITY

A conventional definition of cybersecurity, one which can be found in government strategies and company handbooks, holds that cybersecurity relates to the protection of information that exists in the digital environment from unauthorised intrusion, acquisition or exploitation.

Yet cybersecurity has taken on a much wider meaning. Governments, institutions, the media and civil society all use the term to refer to a broad range of situations. Consider the following, all of which might be classed as cybersecurity concerns:

- A phishing attack leads to hundreds of unsuspecting people revealing their bank log-in details
- A **vulnerability** in software allows access to servers' private keys and users' cookies and passwords
- A hospital's compromised information system makes it impossible to access patient data
- Malware causes a power outage, plunging a city into darkness
- A terrorist cell plots an attack via a hidden network
- A city's water supply becomes unsafe after a **hack** enables unauthorised remote control of a water supply plant
- A copyright-infringing video is uploaded onto a website
- A drug ring uses a crypto-currency to trade illegal narcotics
- A comment insulting a political leader is posted on a social media network

The term can also be used to justify policy measures that undermine human rights. For example, cybersecurity is often invoked by governments to justify restrictions on internet browsing, controls on the use of anonymisation tools and encrypted services, and the extension of police and intelligence powers to conduct surveillance (see pages 26-27 for more detailed information on how these policy measures can undermine human rights).

In the absence of agreed definitions of cybersecurity, how it is framed depends on who gets to frame it. Acts which would be understood as protected speech in some contexts (insulting a political leader, for example) can easily be classed as cybercrime due to definitional ambiguity. So perhaps the more relevant question to ask is: who decides what cybersecurity is and isn't? And where do they decide?

Compared to other policy issues that may have an impact on human rights, cybersecurity poses a particular conceptual challenge. In part this relates to the nature of 'security' itself. Security is impossible to fully achieve or perfect. Because of this, cybersecurity is a state of being which is constantly shifting and can be shaped by policymaking.

THE FREEDOM ONLINE COALITION'S WORKING GROUP ON 'AN INTERNET FREE AND SECURE'

The Freedom Online Coalition's Working Group On An Internet Free And Secure (see page 93) has proposed a definition of cybersecurity which centres the security of the person, as well as systems: "Cybersecurity is the preservation – through policy, technology, and education – of the availability, confidentiality and integrity of information and its underlying infrastructure so as to enhance the security of persons both online and offline."

The diversity of the stakeholders implicated in cybersecurity also poses a challenge. It is an issue for government actors, inter-governmental institutions, technical communities and academia, private sector and civil society (see pages 17 to 22). In the absence of a stable definition, the term has become incredibly broad – referring to phenomena ranging from cross-border **cyber-attacks**, to spam, to technical standards for voting systems.

WHAT HAPPENS WITHOUT CYBERSECURITY

If we think of security as freedom from danger or harm, one of the most important drivers of cybersecurity policymaking is how harms are understood in cyberspace. Without proper cybersecurity measures in place, the possibility of harms arising increases. These are broadly understood to include:

- Theft of data for commercial gain – for example theft of credit card numbers, or theft of personal data for use in spamming or for purposes of identity theft
- Access to data for industrial espionage and the acquisition of competitive advantages
- Theft of data for the purpose of doing reputational harm, to discredit a government or business entity, or to discredit an individual or group of individuals
- Access to data for the purpose of intelligence gathering by a foreign state or non-state entity
- Alteration or deletion of data for commercial, political or economic reasons
- Loss of control over networks as a result of attacks designed to weaken or disable a government or corporate entity
- Manipulation of user behaviour, with users being induced into downloading **malware** or inadvertently taking other harmful actions
- Threats to employees or the public as a result of attacks designed to impair the functioning of public utilities

CYBERSECURITY MEASURES

Despite lack of agreement over the terms and issues being addressed, measures are taken all the time to address the harms outlined above. These may be categorised as follows:

- Technical measures to improve the security of hardware and software that constitute information systems and networks. These may take the form of testing conformity against technical standards such as cryptographic techniques, identity and access management, supply chain risk management, and software assurance.
- Legal measures play a role in regulating the conditions under which personal information is acquired, retained, processed and shared by both private and public sector institutions. Relevant legal measures include data protection law (see pages 40-45), information sharing legislation such as the US Cybersecurity Intelligence Sharing Act (CISA), as well as cybercrime legislation.
- Process-related measures include procedures, guidelines, institutional decisions and educational materials designed to minimise the role people – separately from computers – play in creating or facilitating cyber insecurities through, for example, social engineering attacks, or poor password strength.

THE DIMENSIONS OF CYBERSECURITY POLICY

We've already explored the origins of 'cyber', the wide-ranging use of the term cybersecurity, the cybersecurity-related harms that inform policymaking, and the measures taken to counter those harms. Now we will look at how and where cybersecurity policymaking actually happens.

To begin to approach this question, some categorisation is necessary. With such a complex issue as cybersecurity, there is no neat or definitive way to do this. Although a degree of crossover is inevitable, these three categories provide one way of understanding cybersecurity policymaking as it is today:

- **Information security:** the development of technical and legal standards and processes designed to protect against unauthorised access to information and communications networks.
- **Cybercrime:** measures designed to detect, prevent and investigate illegal activities. This includes both online crimes and offline crimes that have an online element. Cybercrime legislation, digital surveillance measures and restrictions on online content all fall within this area.
- **Cyber conflict:** laws and policies which seek to govern, curtail or regulate the use of **cyber-attacks**, cyber operations, cyber vandalism and cyber theft as perpetrated by or against state actors. This area of policy relates to the development of 'cyber norms', or the effort to translate international law on state conflicts into an online context.

We'll expand on each of these policy areas in Chapter 2 (Information security), Chapter 3 (Cybercrime) and Chapter 4 (Cyber conflict), looking at the different policy measures taken in each, what their human rights implications are, and what human rights defenders should be focusing on.

Want to know more about internet governance? Click here to read our TRAVEL GUIDE TO THE DIGITAL WORLD: Internet Policy and Governance for Human Rights Defenders.

CYBERSECURITY STAKEHOLDERS AND THE CHALLENGES THEY FACE

STAKEHOLDERS

Just as there's more than one way of understanding cybersecurity, there's more than one type of actor involved in making cybersecurity policy.

While it would be impossible to enumerate all of them, at a very general level we can identify five broad categories of actors engaged in cybersecurity policymaking: government actors; inter-governmental institutions; technical communities and academia; private sector; and civil society.

CHALLENGES

Each of these stakeholders faces a range of distinct challenges in their efforts to deal with cybersecurity. Since these challenges shape and guide their actions, identifying them is crucial for any human rights defender engaging with cybersecurity policymaking.

GOVERNMENT

ACTORS

Although arguably every arm of the government now deals with cybersecurity in some way or another, the organisations primarily charged with responsibility for cybersecurity include:

- National technical standards bodies, charged with setting and maintaining technical standards applicable to information security. In the USA, the relevant body is the US National Institute of Standards and Technology (NIST).
- Computer Emergency Response Teams (**CERTs**), also known as computer emergency readiness teams and Computer Security Incident Response Teams (**CSIRTs**). These expert groups – often housed within law enforcement or intelligence agencies –respond to and seek to avert computer security incidents, and are often also tasked with raising public awareness.
- Defence ministries, which are increasingly considering the prospect of cyber conflict and how to engage in it.
- Interior or national security ministries, which generally have oversight over law enforcement and intelligence agencies, coordinate the production of national cybersecurity strategies, and oversee the cybersecurity of critical infrastructure.
- State or foreign ministries, which coordinate foreign policy and negotiations regarding cybersecurity and human rights policy.
- Finance ministries, which manage the budgets for cybersecurity policy.
- Law enforcement agencies, which police not only cybercrime (such as identity theft, child online exploitation, and the sale of illicit goods) but also offline crime with an online element; for example, activities planned using encrypted messaging.
- Intelligence agencies, which generally have responsibilities encompassing the detection and prevention of cybersecurity incidents and the maintenance of critical infrastructure. Intelligence agencies may also undermine cybersecurity, as particular digital surveillance tools (such as **malware**) exploit and manipulate **vulnerabilities** in systems and networks. This is a good example of how governments can take contradictory actions regarding cybersecurity.

CHALLENGES

- The difficulty of digitising government services to make public service delivery more effective, while at the same time having to build the technical capacity and knowledge of government agencies and civil sector employees.
- The absence of sufficient numbers of skilled technologists and security engineers to design and deploy cybersecurity strategies.
- Risks emerging from the cross-jurisdictional nature of cybersecurity, which mean countries with weak cybersecurity resilience strategies can undermine the cybersecurity of all other states.
- The use of anonymisation tools – for example block chain currencies or **encryption** - in crimes involving the internet, which makes policing difficult.
- The constant emergence of new technologies and systems, requiring updated surveillance systems.
- New types of communications services providers, which are often domiciled in other jurisdictions, and require different treatment to traditional telecommunications companies.
- New forms of cybercrime, such as the use of **ransomware**, identity theft, grooming and cyber harassment.
- The necessity of dealing with **cyber-attacks** and other forms of inter-state conflict in the absence of agreed international norms and rules governing state behaviour.

TECHNICAL COMMUNITIES & ACADEMIA

ACTORS

Worldwide, there are more than 200 standards development organisations (SDOs) developing technical standards relevant to cybersecurity. Some of the more prominent ones are:

- International Organisation for Standardisation (ISO), the international gathering of national technical standards bodies.
- Internet Engineering Task Force (IETF) is an open standards organisation with no formal membership requirements which develops and promotes voluntary internet standards, particularly those which comprise the internet protocol suite (TCP/IP). Anyone can take part in the IETF and decisions are consensus-based. There is a working group set up to deal specifically with security as well as a research group looking into implications for human rights on the technical layer (see page 50).
- Internet Architecture Board (IAB) oversees the IETF, and is the committee charged with oversight of the technical and engineering development of the internet. It was originally a US government body but transitioned to independence in 1992. In addition to providing oversight on network protocols and procedures, the IAB works with the Internet Corporation for Assigned Names and Numbers (ICANN).
- ICANN is a non-profit organisation responsible for coordinating the maintenance of several databases of unique identifiers related to the namespaces of the internet. Most visibly, ICANN administers the Domain Name System (DNS), top-level domains, the operation of root name servers, and the assigning of internet protocol address spaces for IPv4 and IPv6.

CHALLENGES

- Ensuring that there is widespread adoption and implementation of agreed voluntary technical standards.
- Overt and covert efforts by states to undermine technical standards or control the process of developing technical standards.

CIVIL SOCIETY

ACTORS

Arguably the least active player in the cybersecurity policy space is civil society. While there is significant and important work being done by human rights defenders in a number of cybersecurity policy areas, there remain areas of cybersecurity policy in which civil society does not substantially engage. Factors contributing to this may include:

- A lack of funding and capacity to follow cybersecurity policy discussions
- The closed nature of many cybersecurity policy forums
- A lack of technical understanding

Civil society is notably engaged on some policy issues overlapping with cybersecurity, including internet governance, privacy and surveillance debates and the intersection of internet issues and freedom of expression. Other groups work on issues like child protection, which are linked closely on cybercrime (see Chapter 3).

CHALLENGES

- The proliferation of government and corporate activities under the banner of cybersecurity, with little clarity as to what is being done and to what end.
- The obfuscation of laws and policies related to the internet, and the lack of transparency around government agencies which monitor and control internet use.
- The lack of transparency around the use by governments of offensive cyber capabilities.
- The rapidly changing nature of technologies, the lack of public understanding and digital literacy (including low levels of use and understanding of privacy-enhancing tools among the general public) and the difficulty of making technical issues accessible to a broad audience.

PRIVATE SECTOR

ACTORS

The internet's infrastructure is largely owned and operated by private entities. Unsurprisingly, these actors have a large stake in cybersecurity:

- Financial institutions are some of the leading developers and promoters of technical standards regarding cybersecurity.
- Software and hardware manufacturers have obligations to ensure security in their products and throughout the supply chain.
- Technology companies and the providers of internet services and applications are often opposed to state measures taken in the name of cybersecurity, or locked in conflict with governments on the question of responsibility and liability for cybercrime. They are increasingly acknowledged as key actors in cybercrime initiatives and the cybersecurity policy space.
- Antivirus and cybersecurity vendors and service providers are crucial for assisting public and private actors in defending against, and responding to, cyber threats. They are also a source of research and data on cybersecurity, for example regarding frequency and types of cybersecurity breaches.

CHALLENGES

- The difficulties of operating across jurisdictions, which include disparate laws, penalties and regulatory regimes.
- Potential for serious reputational damage and possible civil liability if subject to, or responsible for, a cybersecurity incident.
- Pressure to assist governments in the pursuit of cybersecurity and the fight against cybercrime and terrorism – which can include policing and reporting content, shutting down networks (see pages 78-79), blocking services, and even compromising the security of their own products to facilitate surveillance.
- Need to build internal capacity on information and network security.
- Incentives not to disclose data on cyber risks and attacks due to concerns around data privacy and the potential reputational damage.

HOW HUMAN RIGHTS RELATE TO CYBERSECURITY

It is often said that cybersecurity is about the protection of information and networks. Both are important from a human rights perspective. But why?

INFORMATION

Information is central to the functioning of our everyday lives. Individuals generate and share enormous quantities of personal data every day, from emails and health data to bank details and employment records. This data, particularly when aggregated, can easily reveal very sensitive details about a person – for example their sexual orientation, political activity, or geographic location.

This data is generally stored, owned and managed by either private sector entities or the government. From a human rights point of view, this carries serious implications. Without proper cybersecurity measures in place, such information can not only be accessed and stolen, but can be deleted, altered and amended.

The US Office of Personal Management **hack** in 2015, for example, exposed the sensitive personal information of 22 million people - including mental health records and details of drug and alcohol abuse. These kind of attacks have a direct impact on human rights, including the right to privacy, and can directly harm people's lives beyond their interactions online. Yet the government framed the hack as a purely diplomatic incident, promising swift retaliation against the foreign government deemed responsible rather than reflecting on whether such amounts of data should have been collected and stored in the first place, given the weak safeguards in place (see page 68 for more examples of personal data breaches).

Apart from personal data in the hands of private sector entities or the government, there is government and corporate data.

Government data is also sensitive, even if it might not relate to one individual as personal data does. It can include information on trade negotiations, foreign intelligence, troop locations, military secrets and court proceedings.

Corporate data can include information on deals, assets, patents and trade secrets.

OPERATION BUCKSHOT YANKEE

In 2008, US military networks run by US Central Command were attacked by a worm which originally entered the system through an infected flash drive that contained malicious code, or malware. The malware uploaded itself onto the system and scanned for data, including top-secret operational plans, which it could then send to a remote controller. It took 14 months to clean the system, and the incident led to the establishment of US Cyber Command.

NETWORKS

Networks are the infrastructures that transmit and store information and facilitate the connectivity of devices.

From a human rights point of view, networks are important because the functioning of every major public and private service depends on their security. This includes cell phone services, electronic payments, banking systems, metro transportation networks, the provision of gas and electricity and the functioning of traffic lights. Efforts to undermine the functioning of these networks can have immediate and direct effects on the lives of individuals, especially as more and more objects and people are connected to the internet.

From this perspective, measures designed to secure information and networks may be seen as a prerequisite to the enjoyment of a range of human rights:

- The right to privacy and the protection of personal information
- The right to freedom of expression and access to information
- The right to freedom of association and assembly
- The right to liberty and security of person
- The rights of children to be free from exploitation and abuse

THE LIGHTS GO OUT IN UKRAINE

In December 2015, Ukraine power company Prykarpattyaoblenergo reported a power outage in the regional capital Ivano-Frankivsk. Two other utilities experienced outages at the same time, but failed to report them. The same malware, BlackEnergy, was identified in all three outages, suggesting that the power outages were attributable to a cyber-attack. Analysis of the malware revealed that it was designed to wipe system memory. The Ukrainian government has accused Russia of perpetrating the attack.

CYBERSECURITY MEASURES: PROVIDING COVER FOR HUMAN RIGHTS VIOLATIONS?

However, cybersecurity policymaking can also have serious negative implications for the enjoyment of human rights. As we've shown above, policy measures are taken with the stated aim of preventing, detecting or investigating threats and crimes in the online space. However, these measures can also curtail the enjoyment of human rights by individual users. Examples include:

- Measures to prevent **anonymity** or confidentiality online, including the restriction of encrypted services. These are often explained as a means of fighting cybercrime, but can chill free expression and seriously impede the ability of individuals to enjoy their right to privacy. Without access to encrypted services, human rights defenders, journalists, minorities and opposition groups are unable to freely associate without fear of detection (see pages 70-74).
- Punitive measures against and restrictions on 'hacktivist' groups in the name of cybersecurity, which are often disproportionate and impede free expression, communication and association.
- The imposition of **mass surveillance** systems, and the compulsory retention and localisation of data, which undermine the essence of the right to privacy and create surveillance societies, deprived of progressive thought, innovation and creativity (see pages 63-70).
- The blocking of content, imposition of internet filters and criminalisation of the use of computer systems to disseminate restricted content, which impedes the free functioning of the internet and amounts to censorship in the name of policing crime.
- Infrastructure manipulation, internet shutdowns and throttling during political events, elections and demonstrations, which threatens users' rights to expression and protest (see pages 78-79).

- The stockpiling of **vulnerabilities** for use in offensive cyber operations, which actually undermines cybersecurity objectives by making information and networks less secure and more prone to attack (see page 72).

Three recent examples illustrate the broad application of cybersecurity in policymaking:

- In 2015 China published a draft Cybersecurity Law that requires service providers to retain users' personal data and **encryption** of key data within China.
- Israel has allotted USD 26 million in cybersecurity funds to digital initiatives aimed at combatting efforts to 'delegitimise' Israel, notably the Boycott, Divestment and Sanctions (BDS) campaign.
- Australia published draft legislation in 2015 designed to avert "[e]spionage and sabotage through **cyber-attacks** targeting Australia's telecommunications networks and facilities" which grants the Attorney-General broad powers to order telecommunications companies to share extensive amounts of information and do "specified things".

This framing of cybersecurity amounts to a wholesale securitisation (see page 28) of the internet. It figures it as a battleground; a space occupied by criminals and terrorists rather than the space for education, communication and emancipation it should be.

The adverse human rights effects of cybersecurity policies may not always be intentional, but they are foreseeable and avoidable, provided governments invest the time, resources and willpower into engaging with human rights. For this reason in particular, it is essential that human rights defenders are at the table when cybersecurity decisions are made.

SECURITISATION

An online search for 'securitisation' will throw up a number of definitions - most of them related to finance. In the cybersecurity policy space, however, the term has a specific and distinct meaning. It comes out of a school of thought within international relations theory, known as the Copenhagen School, whose adherents define themselves as 'constructivists', and who are interested in how certain situations come about and why, or how what we may perceive as 'reality' is socially constructed.

According to Copenhagen School theorists, securitisation is the process by which certain actors (known as securitising actors) transform an issue into a security issue. The issue, once framed in this way, may then attract a share of attention and resources disproportionate to the threat it represents, and justify extraordinary security measures - for example, a state of emergency or internet shutdown. This theory is often used to explain why some threats to human life - for example terrorism - receive more attention than others in the media and policymaking.

The School identifies the following key features of threats that are securitised:

- They are framed as not merely harmful but dire, imminent and existential (that is to say, a threat to human existence or survival)
- They are framed as a threat to national sovereignty and political autonomy
- The protection of collective survival and values is emphasised over the protection of individuals

There are many potential 'securitising actors' involved in the process, which may include government officials, other policy makers, corporate personalities or lobbyists, and media.

WHAT A HUMAN RIGHTS BASED CYBERSPACE WOULD LOOK LIKE

In June 2012, the United Nations Human Rights Council declared in a resolution that all "the human rights people have offline must also be protected online". Since this landmark moment, however, the UN, its various bodies, and other regional human rights mechanisms, have been slow to provide further guidance on what is required by states in order to ensure this.

This is an evolving area of human rights law, and there are few definitive answers as to what governments and private actors should and should not do when it comes to cyberspace. However, a number of key instruments and judgements (see page 31) offer some guidance on the issue. They mandate that any measures – including those adopted in the name of cybersecurity – resulting in the restriction of human rights in the digital era must meet the following standards:

They must be prescribed by law

It is not enough for measures prohibiting activities on the internet or the use of certain services to be contained in policies or agreements with service providers. They must be provided for by legislation that is precise, public and transparent. Furthermore, their application must be supervised by a judicial or independent body. In the case of secret surveillance, because of the high risk of arbitrary implementation of surveillance measures, judicial authorisation is required.

They must be necessary in a democratic society

Necessary means more than just 'useful' or 'desirable'. It may be useful to prohibit the use of end-to-end **encryption**, but that does not make it necessary to achieve cybersecurity objectives. In the case of secret surveillance, the 'strict necessity' of the surveillance measures should be demonstrated: they should be strictly necessary in a general sense for the safeguarding of democratic institutions, as well as particularly necessary for a particular operation.

They must be a proportionate response to those objectives

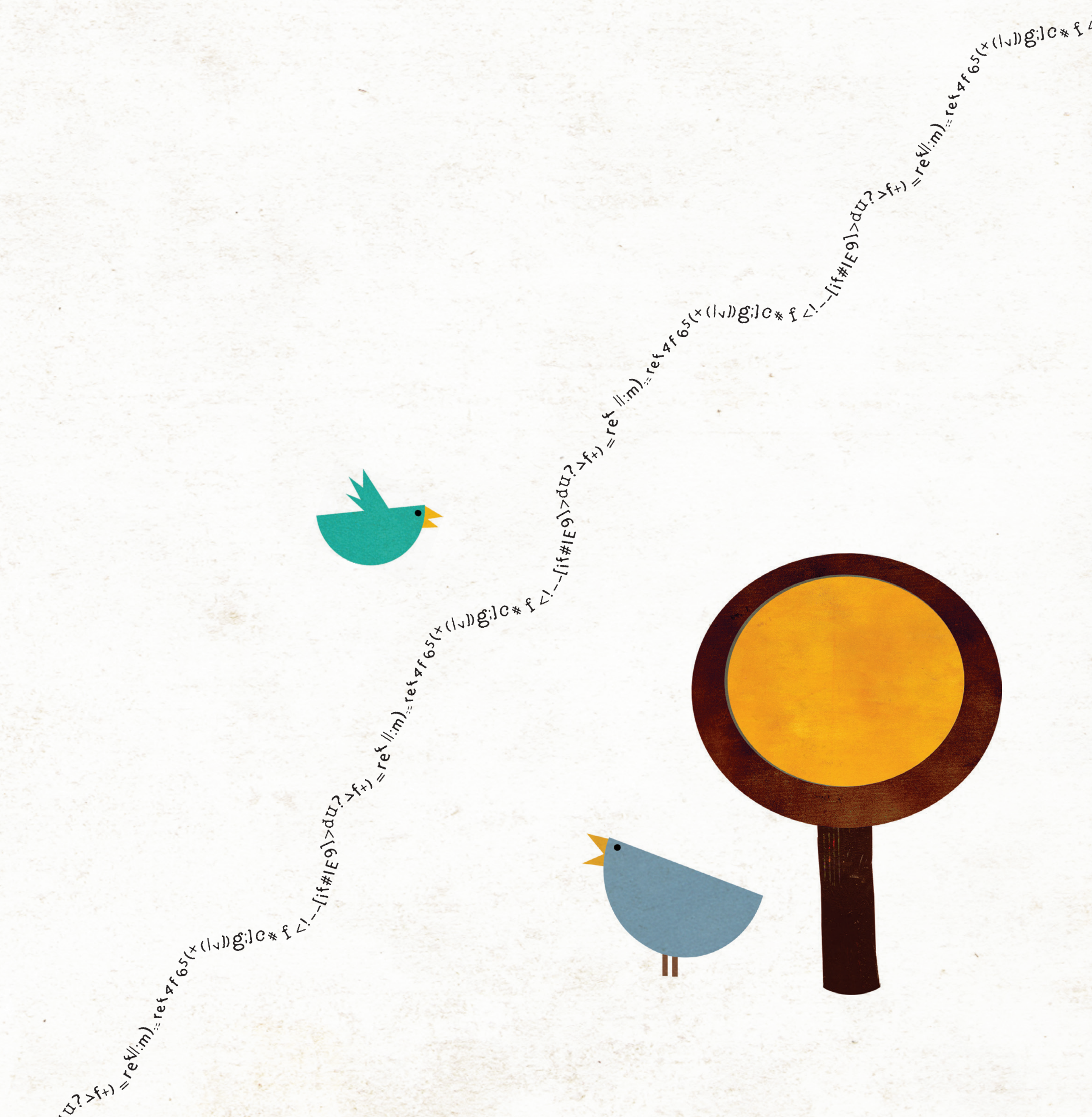
The harm caused by a proposed restriction must not outweigh the benefit gained. When considering the harm caused in the context of restrictions that apply to the internet, it is critical to recall the central role that the rights to freedom of expression, association and assembly play in ensuring a functioning and accountable democracy, and that restrictions applied to the internet can have an incredibly broad application, affecting people all around the world. Where a restriction has a broad impact on individuals who pose no threat to cybersecurity, the state's burden to justify the restriction will be very high.

Where there are less intrusive measures that would achieve the same objective, they must be used and an evidence-based public justification for the restrictions must be provided. Targeted measures are preferable to blanket measures and a proportionality analysis must take into account the strong possibility that encroachments on **encryption** and **anonymity** will be exploited by the same criminal and terrorist networks that the limitations aim to deter.

HUMAN RIGHTS IN CYBERSPACE – KEY INSTRUMENTS, TEXTS AND CASES

- UN General Assembly Resolution A/RES/57/239 on the creation of a global culture of cybersecurity, January 2003.
- UN Human Rights Council Resolution A/HRC/20/L.13 on the promotion, protection and enjoyment of human rights on the internet, June 2012.
- UN General Assembly Resolutions A/68/167 and A/69/166 on the right to privacy in the digital age, December 2013 and December 2014.
- Decision of the Court of Justice of the European Union in joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, Judgment of 8 April 2014, which invalidated the EU Data Retention Directive 2006/24/EC. They held that blanket retention of communications data without any distinction on the basis of geography, commission of a crime, duration, etc. – and in the absence of an objective criterion for access to such data – is a disproportionate interference with privacy.
- Decision of the Grand Chamber of the European Court of Human Rights in *Zakharov v Russia,* Judgment of 4 December 2015, on communications surveillance, which established that surveillance must be based on the existence of a reasonable suspicion, targeted at an individual or premises, and that service providers should receive copies of surveillance warrants.

- Decision of the European Court of Human Rights in *Szabo and Vissy v Hungary*, Judgement of 11 January 2016, on communications surveillance, which established that judicial authorisation should be the norm, and ministerial authorisation the exception; which reiterated the finding in *Zakharov* of the need for individualised reasonable suspicion; and which clarified the need for the demonstration of 'strict' necessity in secret surveillance cases
- Report of the UN High Commissioner of Human Rights A/HRC/27/37 on the right to privacy in the digital age, June 2014, which explored issues of digital and **mass surveillance.**
- The following reports of the Special Rapporteur on freedom of opinion and expression:
    - On the right to freedom of expression on the internet, 2011 (Human Rights Council A/HRC/17/27; General Assembly A/66/290)
    - On the rights to freedom of expression and privacy in the context of communications surveillance, 2013 (A/HRC/23/40)
    - On **encryption** and **anonymity** and the rights to freedom of expression and privacy, 2015 (A/HRC/29/32)
- The International Principles on the application of Human Rights to Communication Surveillance ('Necessary and Proportionate Principles')
- The Manila Principles on Intermediary Liability



CHAPTER II

CYBERSECURITY AS INFORMATION SECURITY

Cybersecurity As Information Security

Information security is about ensuring that data which is created, collected, generated, processed or stored by private and public entities is protected from unauthorised access, tampering, theft and exploitation.

In this sense, cybersecurity is about taking steps to make information and networks more secure. How does information become more secure? That depends in large part on who or what you're trying to secure it from, and what measures (technical, legal, or process-related) you're using to secure it.

A DIFFERENT UNDERSTANDING OF INFORMATION SECURITY

As explained in Chapter 1 (see pages 12-13), the lack of agreed definitions mean that terms are appropriated by different actors for different ends and the term 'information security' is no exception.

China and Russia have previously proposed an International Code of Conduct for Information Security which calls for international cooperation to curb "the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment."

Each government agency, business or other entity will encounter different forms of risk depending on what information they hold and process, for what purpose, and in what manner. For example, a hedge fund might perceive the greatest risk to its cybersecurity to be the theft of confidential information on trades and the manipulation of financial markets, while the disclosure of the personal information of its employees might be considered to be a lower risk.

Each government agency, business or other entity will encounter different forms of risk

A tax authority would consider access to personal data and tax records to be of the highest risk. Indeed, two **cyber-attacks** on the US Internal Revenue Service (IRS) in 2015 and 2016 resulted in the acquisition by 'identity thieves' of more than 100,000 PIN codes used to access taxation files.

> *"Technological innovation during the next few years will have an even more significant impact on our way of life. This innovation is central to our economic prosperity, but it will bring new security vulnerabilities. The Internet of Things will connect tens of billions of new physical devices that could be exploited. [...]"*
>
> Director of National Intelligence James Clapper speaking to the US Senate Armed Services Committee on 9 February 2016

In a threat assessment to the US Senate Armed Services Committee, Director of National Intelligence James Clapper spoke first and foremost of the risks posed by unsecured information systems and networks. Governments and companies all around the world are united in the opinion that cybersecurity, as information security, is a clear and preeminent policy priority. However, a number of debates continue to rage about the best way to achieve this objective.

INTERNATIONAL TECHNICAL STANDARDS

There are more than 1000 publications purporting to set technical standards on cybersecurity - but not a single one comprehensively covers its totality.

This has resulted in the piecemeal and uneven development of technical standards. A US National Institute of Standards and Technology (NIST) report from December 2015, which identifies ten core areas of cybersecurity standardisation (including, for example, cryptographic techniques) notes that across key applications such as cloud computing, emergency management or voting, for the most part only some standards are available, with standards either absent or still being developed in many areas. Technical standards are available in only a handful of select areas of standardisation, such as network security for voting applications.

ISO STANDARD 9564 – PERSONAL IDENTIFICATION NUMBER (PIN) MANAGEMENT

One example of a technical standard is ISO 9564, which relates to PIN management and security in retail banking.

Maintaining security in modern banking systems relies on interoperability between banks, retailers and card issuers, necessitating a common set of rules and practices as to how PINs are acquired, authenticated and transmitted.

This ISO standard provides those rules and practices: from the length of PINs and the specification of PIN entry devices, to PIN issuance and encryption.

Standards development has traditionally been driven by the market and been reactive rather than anticipatory. Standards are developed by Standards Development Organisations (SDOs) around the world, primarily voluntary organisations made up of private individuals, experts and company representatives, which work by consensus. In this way, standards development is often a bottom-up, rather than top-down, process. However, in some countries national standards bodies are heavily influenced by the government. There is a marked difference in approach between the USA, which relies heavily on the private sector to drive standards development, and the European Union, which takes a more top-down approach (for example through the European Telecommunications Standards Institute).

There are more than 1000 publications purporting to set technical standards on cybersecurity - but not a single one comprehensively covers its totality

There is little disagreement about the essential role played by SDOs in standards development for cybersecurity, nor on what the objective of standards development should be. However, the process of negotiating standards development for cybersecurity can be slow, not to mention opaque and closed to the involvement of outsiders. The environment, according to NIST, is increasingly politicised, as countries have begun to 'forum shop' specific public policy interests around different SDOs, viewing the process of standards development as a good opportunity to encourage the adoption of policies that reflect particular agendas.

In addition to the absence of coherent standards, private sector entities also complain of a perceived lack of information and guidance relating to the implementation of standards, and a lack of clarity on what standards to comply with to best suit their organisational demographic and needs. In addition, it can be difficult for them to know which standard or guidance to refer to for 'best practice'. Private sector companies are overwhelmed with standards in certain areas, and significantly underserved in other areas, such as standards relating to how employees and contractors should act to protect cybersecurity.

Indeed, there is an overemphasis on technical standards to the exclusion of process-related standards (see page 15). A study commissioned by the UK government in 2015 revealed that there are more than 1000 publications on cybersecurity globally, 67 percent of which focus on organisational cybersecurity standards, and only 3 percent on cybersecurity and individual security.

COHERENCE OF LEGAL OBLIGATIONS AND RESPONSIBILITIES

The legal landscape of cybersecurity is marked by absence. There is no agreed global framework for data protection. There is no coherence on the sharing of information between private and public sector entities for the achievement of cybersecurity – as well as national security and law enforcement – objectives. For global organisations operating across a variety of markets, these factors increasingly impede the adoption and implementation of cybersecurity strategies.

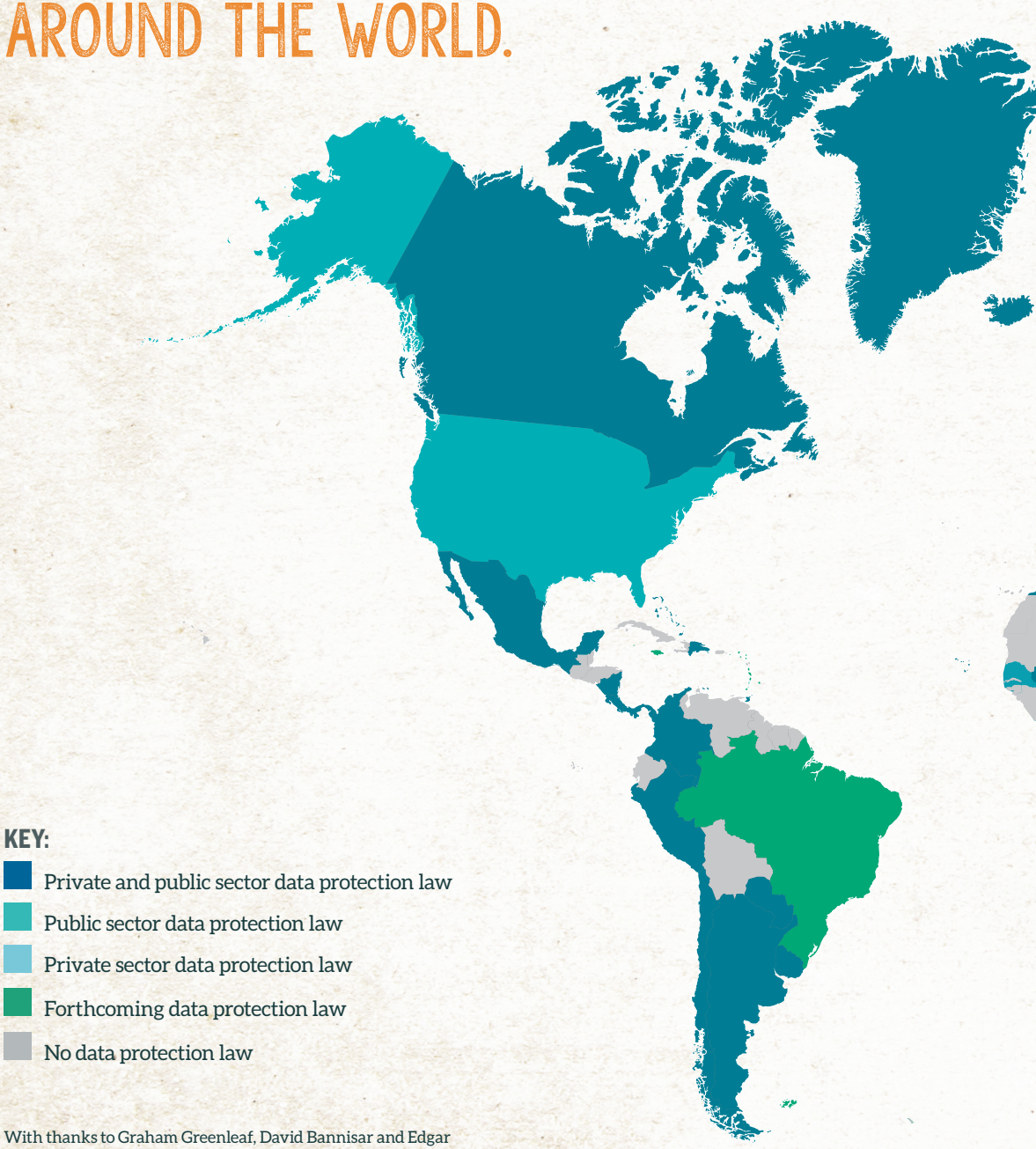
The absence of global – and, particularly, transatlantic – agreement on data protection standards was brought into focus with the decision of the Court of Justice of the European Union in *Schrems v Data Protection Commissioner* on the Safe Harbour Agreement in 2015. The case invalidated the legal basis on which companies could transfer data collected in the EU to the USA for processing.

At the heart of the decision were questions around the disparity between EU and US data protection and privacy protections, but the judgement has global ramifications. As businesses in Europe look to outsource business process tasks to countries beyond European borders, the privacy and data protection regimes in Asia, Latin America and Africa will increasingly standardise their regulatory frameworks with Europe.

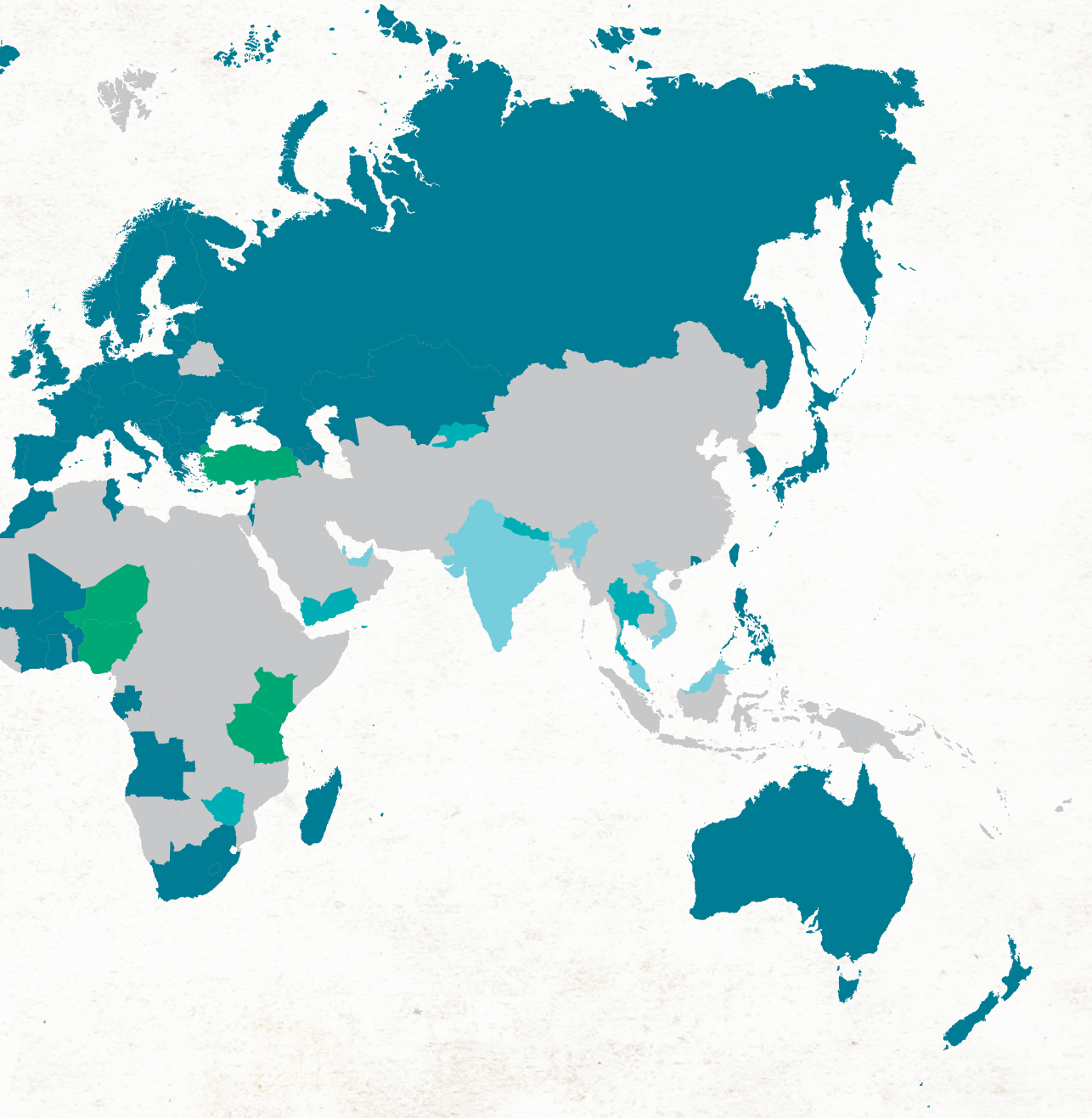
Private sector companies are overwhelmed with standards in certain areas, and significantly underserved in other areas

Following the Court of Justice's ruling, the EU and the USA entered a process of adopting a successor to the agreement, known as the Privacy Shield. However, a longer term solution to the disparity in approaches to data protection may be needed. Europe has long taken an active regulatory approach to the protection of personal data, whereas the USA has preferred self- and sectoral regulation regimes. This creates numerous compliance headaches for companies operating in both jurisdictions. As the number of companies operating cross-jurisdictionally multiplies, and other countries around the world adopt legislation mimicking the EU approach, the business case for a global agreement on data protection only becomes stronger. The EU and the USA concluded an Umbrella Agreement on Data Protection in September 2015, designed to apply to the transatlantic transfer of data between government agencies (rather than corporate entities), which is arguably the first step towards standardisation of the two regimes.

DATA PROTECTION LAWS AROUND THE WORLD.



With thanks to Graham Greenleaf, David Bannisar and Edgar Whitley for providing the data which underpins this map.



INFORMATION-SHARING PRACTICES

In 2015, both the USA and Europe adopted legislation pertaining to the disclosure of information by corporate entities and between government agencies for cybersecurity purposes. The US Cybersecurity Information Sharing Act (CISA), signed into law in December 2015, enables internet companies and other private sector entities in the USA to share internet traffic information with the US government, especially in the case of cybersecurity threats. The Act has been strongly criticised by human rights defenders and civil society organisations, concerned about the law's extension of blanket immunity from civil and criminal penalties to companies sharing personal information without a warrant. The Act allows for data to be shared with a wide array of government agencies, from the FBI and NSA to the Internal Revenue Service. In an environment already marked by concerns over the accountability and transparency of US intelligence agencies, many fear CISA will function as another form of surveillance. Yet the government argues that it is necessary to encourage corporate entities to share data that is essential in detecting and preventing cybersecurity threats.

In 2015 two unprecedented initiatives signalled a new era of regulation regarding obligations to report and respond to cybersecurity incidents

In the same month CISA passed, the European Union reached agreement on the Network and Information Security (NIS) Directive. This Directive not only requires the establishment of national cybersecurity strategies, but imposes obligations on operators of essential services (e.g. transport or financial services) and digital service providers to report cybersecurity incidents to national authorities.

These two unprecedented initiatives signal a new era of regulation regarding obligations to report and respond to cybersecurity incidents.

THE FIVE EYES AGREEMENT

Whereas police forces generally have to go through formal – and often unwieldy – legal processes in order to procure information from, and share information with, other police forces around the world, intelligence agencies often have a much more fluid and integrated relationship with their foreign counterparts. This is particularly true of the spying agencies of the USA, the UK, Australia, New Zealand and Canada, which operate in an alliance known as the Five Eyes.

Underpinned by a series of multilateral and bilateral memoranda of understanding beginning in 1946, known collectively as the Five Eyes Agreement, the signals intelligence agencies of these five countries operate in a highly integrated manner, sharing raw surveillance data, undertaking joint spying and hacking operations, even maintaining staff in each others' facilities.

With the publication of documents leaked by NSA whistleblower Edward Snowden, the Five Eyes Agreement has been put under greater scrutiny. However, the exchange of intelligence information still remains shrouded in secrecy, and obscured from public scrutiny. Organisations like Privacy International have repeatedly called for the full public disclosure of intelligence sharing agreements – not only of the Five Eyes Agreement, but of similar arrangements around the world. For more, see Selected Resources.

THE CROSS-BORDER TRANSFER OF DATA

The final policy area related to the coherence of information sharing pertains to the cross-border transfer of data for law enforcement and intelligence purposes. This is an increasingly problematic and complex area of policy in the national security and law enforcement field. Where traditionally police and intelligence agencies were able to access data held by companies (particularly regarding communications) relatively easily because those companies were based in their jurisdiction, today a large majority of individuals use communications services which are based abroad, particularly in the USA.

In order to give effect to warrants or orders requiring access to corporate data, states now have to rely on a range of bilateral Mutual Legal Assistance Treaties (MLATs) as well as intelligence sharing arrangements like the Five Eyes Agreement (see page 45). This is not only impeding the efficiency of investigations – most requests made via the MLAT process will take up to a year to be completed – but it is creating incentives for states to circumvent such processes using interception and other surveillance techniques.

The Council of Europe Convention on Cybercrime (the Budapest Convention, see page 58) contains provisions allowing parties to obtain transborder access to stored computer data with consent or where publicly available (Article 32). The provision is designed to allow unilateral access by one party to data held in another party's jurisdiction, and thus constitutes a workaround or exception to MLAT processes. The question of transborder access is an incredibly controversial one, not least because Article 32 can be interpreted as allowing for remote search and seizure (also known as intrusion or **hacking**), and was cited by states such as Russia as a reason for not joining the Convention – on the rationale that it violates the principle of sovereignty.

In 2013, the Council of Europe proposed an Additional Protocol to the Convention on Cybercrime regarding transborder access to data, but later concluded that such a proposal would not be feasible. In the intervening months, the Snowden revelations of US and UK surveillance were published, transforming the debate on law enforcement and intelligence access to personal data. A 2013 report by the Cybercrime Convention Committee's sub-group on jurisdiction and transborder access to data said that new developments also made it necessary to revise the reach of Article 32b, noting that "current practices regarding direct law enforcement access to data [...] frequently go beyond the limited possibilities foreseen in Article 32b and the Budapest Convention in general," posing risks to human rights.

It is in the interests of every state to support the development of capacity within other governments to detect and respond to cybersecurity threats

CERTs AND CSIRTs

A final policy priority in the field of information security is building the capacity for private and public actors to manage and respond to cybersecurity incidents. Because cybersecurity does not stop at borders, it is in the interests of every state to support the development of capacity within other governments to detect and respond to cybersecurity threats. The primary actors devoting resources to the capacity building of Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) are international organisations like the Organization of American States (OAS) and the Commonwealth Telecommunications Union (CTU), and large foreign aid donors such as the USA and the UK.

COORDINATION IN CYBERSPACE: THE UK AND THE USA RESPOND TO GAMEOVER ZEUS BOTNET

Responding to cyber-attacks is a challenge for even the most well-equipped law enforcement agencies, as the USA and the UK recently demonstrated when addressing the GameOver Zeus botnet, a network of computers used to steal millions of dollars from individuals all around the world. Although impressive coordination led to the detection of the botnet, the way information was released to the public was problematic.

After the botnet was identified, the British National Crime Agency (NCA) released a press release, urging people to take steps to "protect themselves against powerful malicious software". What 'steps' people should take, beyond visiting the Get Safe Online website, were not clear. When the website collapsed - possibly under the weight of the traffic - chaos ensued.

The UK CERT added to the panic by reissuing the NCA's warning, encouraging people to use antivirus and anti-malware tools and change their passwords. At no time did the CERT inform the public that only Windows software was affected and there has been no subsequent information issued since.

Source: http://www.bbc.com/news/technology-27681996.

Cybersecurity capacity building is an area around which significant cooperation is visible, particularly at the regional level. The Association of Southeast Asian Nations (ASEAN), for example, adopted the Singapore Declaration in 2003 which urged member states to develop and operationalise national Computer Emergency Response Teams (**CERT**s) by 2005. The new EU Networks and Information Security (NIS) Directive requires member states to adopt a national NIS strategy defining the strategic objectives and appropriate policy and regulatory

measures in relation to cybersecurity. Member states will also be required to designate a national competent authority for the implementation and enforcement of the Directive, as well as Computer Security Incident Response Teams (**CSIRT**s) responsible for handling incidents and risks. The EU also conducts emergency trainings and holds EU-wide cybersecurity awareness days.

National education and public awareness programmes are essential to educating individuals about cybersecurity

In addition to international capacity building, national education and public awareness programmes are essential to educating individuals about cybersecurity. Initiatives such as Canada's 'Get Cyber Safe' programme and Australia's Cybersmart website are designed to increase general awareness of the impact and origins of cybersecurity threats.

RECOMMENDATIONS FOR HUMAN RIGHTS DEFENDERS

Engagement with information security policymaking is necessarily limited by the often highly technical nature of the issues. However, there is much that human rights defenders can do to ensure that human rights are brought into these discussions.

1. Monitor and engage with Standards Development Organisations (SDOs) to ensure they remain neutral and do not become politicised in a way that places human rights at risk.

Having technical standards in place for cybersecurity is consistent with the protection of the rights to privacy, freedom of expression and security. To make sure these standards are rights-respecting, it is vital that civil society monitor and engage with SDOs.

There are several ways to do this. At the organisational level, civil society can attend SDO meetings, put human rights concerns on the agenda, and provide educational material to meeting participants, highlighting the links between the development of technical standards and human rights. The Human Rights Protocol Considerations Research Group at the Internet Engineering Task Force (IETF), and ICANN's Cross Community Working Party on its Corporate and Social Responsibility to Respect Human Rights, are examples of spaces where civil society can input.

Where there are no formal opportunities for engagement at the organisational level, civil society can also reach out to SDO members individually. In a large SDO like the International Organisation for Standardisation (ISO), this would mean reaching out to the national representative organisation from the civil society group's respective country.

The leadership of SDOs can have a strong influence over the position taken by the SDO on particular standards. Civil society should therefore monitor appointments to ensure they do not compromise the independence of the SDO – for example, if they are put forward by a particular country for strategic reasons. Candidates for SDO leadership positions should have the requisite technical background and demonstrate a clear understanding of the human rights implications of cybersecurity standards development.

2. Advocate for adequate resources to be provided to public and private entities to ensure they can adopt and conform with technical standards that provide the highest level of information security.

Supporting measures to improve cybersecurity should be viewed as part of a state's obligations to provide the conditions for enjoyment of the rights to privacy, freedom of expression, and security. Governments have a responsibility to invest

in cybersecurity measures that comply with human rights. Relevant ministries should be educated about the links between cybersecurity and human rights and encouraged to view budgetary investment in cybersecurity as a prerequisite to meeting human rights obligations.

3. Advocate for robust data protection and privacy legislation around the world.

There are too few human rights groups engaged in data protection, and public awareness about the links between data protection and human rights is low. Data protection law should be viewed as a pillar of any functioning democracy, and those countries without comprehensive data protection legislation – including India, China, the United States, and most African countries – should be encouraged to adopt it. Where data protection law exists, advocacy should focus on ensuring it is fit to deal with the wide array of information security issues in existence.

4. Campaign for transparency around the implementation of information sharing for cybersecurity agreements, to ensure that they do not result in an undue amount of private information being shared between governments and companies.

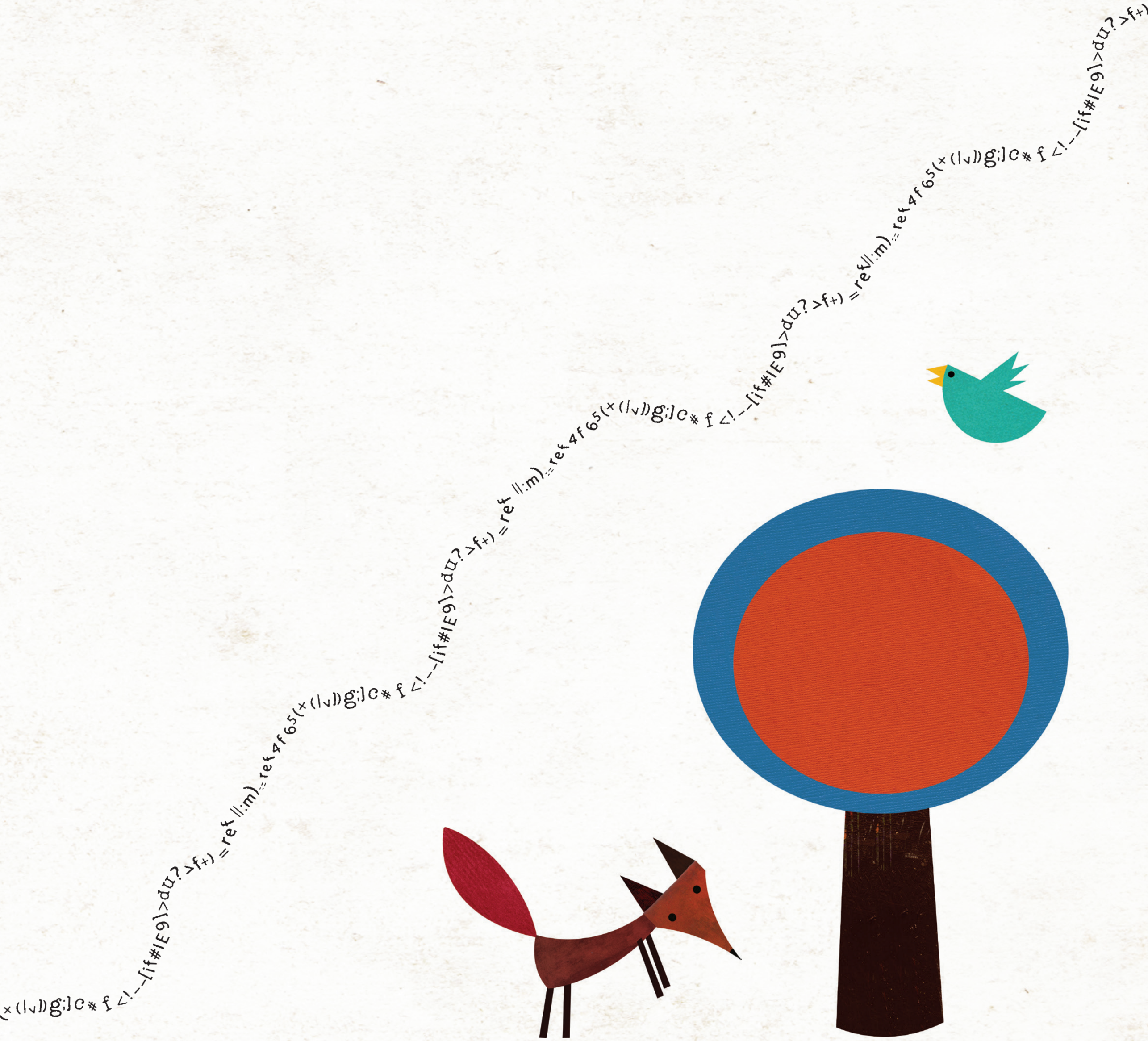
Increasingly, governments are adopting laws requiring the disclosure of information on cyber threats from the private sector. The lack of transparency around such cooperation, conducted under the auspices of national security and cybersecurity, must be rectified; it is only through public scrutiny that governments and companies will be held accountable. Human rights defenders should campaign for governments and companies to publish details about the amount and type of information that is shared under cybersecurity information sharing agreements.

5. Monitor the negotiation of cross-border data sharing agreements to prevent the deterioration of human rights safeguards.

Human rights defenders must demand that negotiations around cross-border data sharing agreements are made as public as possible to ensure negotiations do not result in the trading away of human rights protections in exchange for greater surveillance powers. Often an extreme degree of secrecy exists around such agreements. In these instances, access to information laws, as well as public campaigning, should be used to inform advocacy.

6. Advocate for the inclusion of human rights at the heart of all cybersecurity capacity building initiatives.

Human rights shouldn't be an afterthought or mere compliance issue – they should be placed at the heart of cybersecurity training right from the outset. Institutions and donor governments involved in foreign capacity building initiatives have a responsibility to share knowledge about the human rights impacts of cybersecurity measures. Human rights defenders could work with such actors in order to devise and execute human rights training and education.



CHAPTER III

CYBERSECURITY AS CYBERCRIME

Cybersecurity As Cybercrime

According to the received definition of cybercrime – crimes that involve computers and networks – everyone from a petty drug dealer messaging his customers using WhatsApp to an art thief using Google Maps to plot his getaway, can be a cybercriminal.

Most people probably wouldn't regard traditional crimes using the internet as a medium as cybercrime. To the average citizen, cybercrime means crimes that can only happen online: the theft of identity data, for example, or the use of ransomware. Yet discourse around cybercrime frequently blurs the line between these two areas of law.

It is hard to imagine a modern day crime that doesn't involve, at some point in its execution, the use of a computer

It would have difficult for the drafters of the world's first cybercrime law, the Budapest Convention, to foresee that cybercrime might one day come to mean 'all crime'. After all, it was 2001 - smart phones had barely been invented and no one could have predicted the extent to which computers would become so deeply integrated into our lives; that they would one day fit into our hands, replace our watches and TVs, and even drive our cars.

Today, cybercrime sits at the centre of policy debates on internet regulation, child safety, government surveillance, policing, and counterterrorism, as well as - critically - cybersecurity.

Four types of criminals dominate cybercrime policymaking discussions:

- **Terrorist groups** whose use of the internet ranges from the basic (use of social media to disseminate terrorist recruitment material, use of messaging apps to communicate) to the sophisticated (use of anonymous routing and anonymous website hosting for planning, recruitment, and dissemination of materials)
- **Paedophiles and paedophilia rings** using the internet to exchange, disseminate, buy and sell child sex abuse imagery, and for grooming children online
- **Organised crime syndicates** facilitating the trade in illicit drugs, weapons, money and stolen goods and information
- **Cyber attackers and hackers** attacking information and networks to acquire, delete or alter information, cause damage and otherwise weaken security

THE REMIT OF CYBERCRIME LAWS

Although the definition of cybercrime is sufficiently broad to extend to other more mundane offline crimes, it is the above listed categories which are most commonly referenced in relation to cybersecurity measures. However, cybercrime laws are generally more restricted in their application to computer misuse, fraud and abuse offences (those targeting cyber attackers and hackers), and content-related offences.

THE BUDAPEST CONVENTION

The Budapest Convention is the authoritative law on cybercrime, and the basis for the laws of its 48 parties. There are three substantive categories of offence:

- Offences against the confidentiality, integrity and availability of computer data and systems (Title 1) and computer-related offences (Title 2). These are those offences primarily related to cyber-attacks and hacking, and include interference with and interception of data. Many countries have incorporated such provisions under the ambit of 'computer misuse' legislation.
- Content-related offences (Title 3). These offences relate to the dissemination of 'child pornography'. The use of the word 'pornography' has been extremely controversial and many states now refer to 'child sex abuse imagery' or 'paedophilia material' instead.
- Offences related to infringement of copyright (Title 4). These offences relate to the infringement of copyright on a commercial scale by means of a computer system.

The Convention outlines a number of procedural requirements to facilitate the investigation of cybercrime and the obtaining of evidence. These include general provisions on extradition and mutual legal assistance, as well as the obligation to legislate for powers compelling:

- Expedited preservation of stored computer data (Article 16), and preservation and disclosure of traffic data (Article 17)
- Production of specified computer data by those who hold it (namely, internet companies and telecommunications providers), specifically subscriber information and metadata (Article 18)
- Search and seizure of stored data (Article 19)
- Real-time collection of traffic data (Article 20)
- Interception of content data (Article 21)

ADDITIONAL PROTOCOL ON RACIST AND XENOPHOBIC ACTS

The content-related offences of the Budapest Convention were subsequently supplemented in 2006 by the adoption of an Additional Protocol, addressing the use of the internet (or, 'computer systems') to propagate racist or xenophobic material. Specifically, the Additional Protocol requires parties to enact laws creating the following offences:

- Distributing, or otherwise making available, racist and xenophobic material to the public through a computer system (Article 3)
- Threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, or insulting, through a computer system, persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors (Article 4)
- Distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity (Article 6)

As of December 2015 the Additional Protocol had been ratified by 24 states (all of them Council of Europe member states). The USA, a key non-Council of Europe party to the Budapest Convention, has refused to adopt the Protocol, noting that the provisions run contrary to US constitutional protections in the field of free expression. Indeed, the Additional Protocol raises grave concerns about the threshold beyond which legitimate speech online becomes hate speech, which can be justifiably restricted under human rights law.

THE CONVENTION AND NATIONAL CYBERCRIME LAWS

During the drafting of the Convention, concerns were raised that "the protection of society against cybercrime" would be used to enact increasingly broad and illegitimate restrictions on online content, and to expand surveillance powers. Although the Convention's stated aim - of standardising disparate national legal frameworks related to computer crime - is an important and valid one, civil society had expressed concerns that it could be used by non-state parties to provide cover for undue restriction of internet use. Indeed, since 2001 there have been numerous instances of states operating in the purported interest of countering cybercrime in order to criminalise online speech and monitor and censor the internet. Some examples of such legislation include:

- **Kuwait's cybercrime law**, passed in 2015, which: contains provisions imposing prison sentences and fines for insulting religion and religious figures, and for criticising the emir over the internet (Article 6); prohibits Internet-based statements deemed to criticise the judicial system or harm Kuwait's relations with other states, or which publicise classified information, without exceptions for disclosures in the public interest (Article 6); and imposes a punishment of up to 10 years in prison for using the Internet to "overthrow the ruling regime in the country when this instigation included an enticement to change the system by force or through illegal means, or by urging to use force to change the social and economic system that exists in the country, or to adopt creeds that aim at destroying the basic statutes of Kuwait through illegal means" (Article 7).
- **The African Union Convention on Cybercrime and Data Protection**, adopted in 2014, which contains provisions criminalising the making, disseminating or downloading of content containing threats or insults on the basis of race, colour, descent, national or ethnic origin, or religion, as well as the participation in online or physical groups "established with a view to preparing or committing" a criminal offence defined in the Convention.

- **Saudi Arabia's Anti-Cyber Crime Law**, which includes reference to the "protection of public interest, morals, and common values" and has been used against bloggers and others for crimes related to insulting public officials, or supporting forces other than the government in power.
- **Tanzania's Cybercrimes Act**, enacted in May 2015, which criminalises any person who publishes information, data or facts presented in a picture, text, symbol or any other form in a computer system where such information, data or fact is false, desceptive [sic], misleading or inaccurate" (section 16).
- **Pakistan's Prevention of Electronic Crimes Bill**, under negotiation in the parliament as of 2015, which criminalises anyone who "prepares or disseminates" any type of electronic communication with the intent to praise a person simply "accused of a crime," or to "advance religious, ethnic or sectarian hatred" (Article 9). The Bill also contains a crime of "cyberterrorism", which includes the "glorification" of crime or unauthorised access to, copying, or transmission of "critical" information with the intent to create a sense of fear or insecurity in the government or the public or to advance religious, ethnic, or sectarian hatred (Article 10). The Bill also creates broad surveillance and data acquisition powers, and powers of government censorship of content when the government considers it "necessary in the interest of the glory of Islam or the integrity, security or defence of Pakistan".

The prospect of cybercrime being used to advance laws restricting free expression, political commentary and genuine critique is arguably the most troubling aspect of cybercrime discourse.

When drafting cybercrime legislation, which requires specialised knowledge and expertise, countries may turn to 'model laws'. However, the use of such laws can be problematic. A study commissioned for the Council of Europe, for example, on cybercrime model laws (see more in Selected Resources) concluded that "The use of such model laws poses risks and serious concerns.

Absence of essential provisions, defective language [...] And their divergence away from and inconsistency with international best practice do a disservice to the goal of achieving greater international cooperation against cybercrime."

HUMAN RIGHTS DEFENDERS FIGHT 'CYBER MARTIAL LAW' IN THE PHILIPPINES

In 2012, the Filipino government enacted the Cybercrime Prevention Act of 2012. The Act was broadly criticised by feminist groups, human rights defenders and journalists for its wide-ranging provisions which criminalised everything from cybersex to libellous speech. NGOs banded together to establish the Philippine Internet Freedom Alliance, organised street protests and filed petitions with the Supreme Court.

The Filipino Supreme Court issued and then extended temporary restraining orders against the implementation of the law until the case was decided in February 2014. At that time, the Court upheld the online libel provision, but restricted its application to cases where it covers persons other than the original author. Recipients of, and internet users who react to, a potentially defamatory post, will not be covered by online libel.

The Court struck down section 4(c) (3) (on unsolicited commercial communications), section 12 (real-time collection of traffic data), and section 19 (restricting or blocking computer data).

The policing of cybercrime is becoming synonymous with crackdowns on expression that challenges the status quo, and increasingly undermines the effectiveness and free functioning of human rights defenders.

A big topic for discussion in the cybercrime policy space is the need for cybercrime laws which cover activities without jurisdictional boundaries.

Currently, due to the limited reach of the Cybercrime Convention (which, as of 2016, does not include China, India, Brazil, or South Africa), cybercrime legislation is not globally harmonised. This poses a problem for states trying to crack down on offences like computer misuse, **hacking**, and **cyber-attack** – if an offence originates in a country which does not criminalise it, it can be difficult or impossible to prosecute.

However, these debates about harmonisation can often quickly segue into the need to harmonise law enforcement and intelligence powers to conduct surveillance, monitor internet activities, block and filter internet content, and crack down on the use of anonymisation tools.

MASS SURVEILLANCE

> *"But a digital society also presents us with challenges. The same benefits enjoyed by us all are being exploited by serious and organised criminals, online fraudsters and terrorists.*
>
> *The task of law enforcement and the security and intelligence agencies has become vastly more demanding in this digital age. It is right, therefore, that those who are charged with protecting us should have the powers they need to do so."*
>
> British Home Secretary Theresa May speaking in November 2015 when introducing the Draft Investigatory Powers Bill, containing mass surveillance and bulk data retention powers.

> *The law on intelligence [...] will strengthen the effectiveness of our preventative measures. We are enhancing the means of our service, including the creation of 1,500 jobs since January [...] These positions will be distributed amongst foreign and internal intelligence, and the fight against cybercrime."*
>
> French Interior Minister Bernard Caeneuve, speaking in July 2015 about the Loi sur le Renseignement, the French surveillance law which contains mass surveillance and bulk data retention powers.

Few human rights issues have attracted as much public debate and political attention in the past few years than state surveillance, and the role of the private sector in facilitating it. More than perhaps another other community, human rights defenders understand the gradual expansion of state surveillance online, and its effect not only on their privacy, but on their ability to confidently and without fear express and organise themselves.

Under the banner of fighting cybercrime, states are developing and expanding mass surveillance programmes

Two particular types of mass surveillance dominate current policy discussions and legislative debates: bulk interception, and mandatory communications data retention.

The increasingly popularity of **mass surveillance** among governments around the world can be attributed to a number of factors, including:

- The rapidly declining cost of technology and data storage, which makes capturing and storing (even indefinitely) data cheaper than ever before.
- The ubiquity of digital devices, which create and transmit extensive amounts of information that can be easily acquired and analysed to track and monitor citizens and foreigners.

- The processing power of computing, which can now analyse, process and derive information from huge datasets with a far greater degree of accuracy than at any other time in history, allegedly limiting the need for human analysis of intelligence.

Above all, however, the clear preference for **mass surveillance** is motivated by a change in mind-set as to the nature of security and the role of surveillance. As cybersecurity and fighting

Want to know more about surveillance? Click here to read our TRAVEL GUIDE TO THE DIGITAL WORLD: Surveillance and International Standards.

transnational terrorism have become the chief drivers of surveillance policy, a particular conceptualisation of modern surveillance has thrived: one which says that all acts of digital communications are potentially necessary pieces of an unwieldy security puzzle - which can only be solved by collecting every piece. Or, to use a more popular analogy: that effective law enforcement and the protection of cybersecurity requires the identification of needles in a haystack, and the only way to identify the needles is to collect every piece of hay available.

Bulk interception capabilities form a key part of the existing and proposed surveillance capabilities of a number of countries. For example:

- Since 2008, the US Foreign Intelligence Surveillance Act section 702 has facilitated the bulk collection of the communications of non-US persons, providing legal coverage for mass surveillance systems such as Upstream. The USA also uses Executive Order 12333 to conduct wholly foreign bulk collection, although little is known about this power.
- India passed the Information Technology Act of 2008, section 89 of which enables the government to intercept, monitor or

decrypt all communication if it is necessary or expedient to do so in the interests of the sovereignty or integrity of India, among other broadly-worded reasons.

- Also in 2008, Sweden adopted the Signals Intelligence Law (also known as the FRA law) which enables the bulk interception of cable communications.
- In 2013, Colombia adopted a law on intelligence which expanded the powers of intelligence agencies to 'monitor' communications on a bulk scale, without authorisation. The country is known to have acquired a number of technical capabilities enabling bulk interception and data acquisition.
- The UK's Investigatory Powers Bill, introduced in Parliament in March 2016, replicates the bulk interception powers in section 8 of the current Regulation of Investigatory Powers Act 2000, and also creates powers to conduct **hacking** and acquisition of datasets in bulk.
- In 2015, France passed two laws which open the door for mass surveillance: the 'Loi du 24 juillet 2015 relative au Renseignement' which, among other things, authorises the installation of 'black boxes' on the infrastructure of telecommunications providers to enable the filtering for terrorist content; and the International Surveillance Law, passed later in 2015 after being separated from the earlier law because of constitutional concerns, which authorises bulk interception of foreign communications.
- In 2015, Switzerland introduced a new surveillance law enabling the tapping of cables for the purposes of bulk interception.
- As of 2016, Finland and Denmark were both considering similar laws.

Bulk interception systems can also be purchased on the private market; French companies Qosmos and Amesys famously sold such technology to Gaddafi's Libya.

Although the Snowden revelations about the bulk interception programmes operated by the USA and the UK caused great uproar, causing UN Special Rapporteur on protecting human rights while countering terrorism, Ben Emerson QC, to conclude that "the very existence of mass surveillance programmes constitutes a potentially disproportionate interference with the right to privacy", states continue to maintain bulk interception is necessary tool for fighting terrorism and cybercrime. In 2016, in at least two countries (the UK and the Netherlands), draft legislation was under consideration that would extend these powers.

The ever-widening gap between international law and state practice raises serious concerns about the protection of human rights, in an increasingly securitised climate (see page 28 for an explanation of 'securitisation'). At the same time as states are expanding surveillance powers, a range of regional and international human rights bodies have declared that bulk interception surveillance measures do not conform with international human rights law, including:

- The UN High Commissioner for Human Rights (A/HRC/27/37)
- The UN Special Rapporteur on protecting human rights while countering terrorism (A/69/397)
- The Court of Justice of the European Union (in *Schrems v Data Protection Commissioner of Ireland*, judgement of 6 October 2015)
- The European Court of Human Rights (in two judgements of December 2015 [*Zakharov v Russia*] and January 2016 [*Szabo and Vissy v Hungary*])

Mandatory data retention is another form of **mass surveillance**. By requiring communications service providers to retain – and sometimes generate – extensive information about an individual's communications, locations and connections, and make such data available to police and intelligence agencies at will, data retention laws constitute a form of pervasive surveillance that can impede online **anonymity** and chill freedom of expression. It also creates additional responsibilities for the service provider retaining the data, which could subsequently be subject to attac ks aimed at stealing or altering data.

THE COST OF CYBER-ATTACKS

A number of high profile cyber-attacks have left companies and organisations suffering both financial and reputational costs:

- A Los Angeles hospital, the Hollywood Presbyterian Medical Centre, paid USD 17,000 in bitcoin to hackers who seized control of the hospital's network with ransomware
- British phone network provider TalkTalk lost 101,000 customers and GBP60 million after the financial details of 156,000 of its customers were accessed in a 2015 cyber-attack
- An attack on Sony Pictures in 2014, purportedly in response to the company's decision to make the North Korean parody film The Interview, may not have had severe financial consequences for the company, but caused significant embarrassment for employees and associates of the companies whose private emails and records were made public for the world. More than 3000 of the company's employees' Social Security numbers were exposed, along with salary information, personnel reviews and medical histories

European data retention laws were spearheaded by the UK, which in 2000 – around the same time that the Budapest Cybercrime Convention was being negotiated – attempted to pass legislation mandating the retention of data for seven years. After repeated failures to get the legislation through parliament, it was pushed through the European Data Retention Directive when the UK held the EU Presidency in 2006. Mandatory data retention then became law throughout Europe.

In the aftermath of the Snowden revelations, and in particular the exposure of the NSA's bulk telephone **metadata** programme, the human rights implications of data retention were given renewed attention. Cases in the USA, Canada, the UK and the Court of Justice of the European Union challenged the casting of metadata as deserving of lower levels of protection under the right to privacy.

In the Court of Justice of the European Union case of *Digital Rights Ireland v Ireland* (2014), brought by the Irish NGO Digital Rights Ireland concerning the validity of the Data Retention Directive, the Grand Chamber noted the dangers of collecting and using personal data in bulk, concluding that the Directive "entails an interference with the fundamental rights of practically the entire European population". It proceeded to invalidate the law on the grounds of proportionality.

The invalidation of the Data Retention Directive cast doubt on the legal basis in EU Member States for requiring the retention of communications data. Various EU Member States abandoned data retention powers, while others re-legislated for them, including the UK (in July 2014) and Germany (in October 2015), although in both countries the new laws are being challenged in court. Elsewhere in the world, Australia adopted data retention laws in March 2015, while the parliament of Paraguay resisted proposed data retention laws in July 2015 – a rare exception. After a number of court cases concerning the NSA's bulk telephone **metadata** programme, section 215 of the Patriot Act expired in June 2015, and was amended by the USA FREEDOM Act, which alters – but does not eradicate – the metadata retention processes.

In the post-Snowden landscape, policy discourse around mass surveillance (both bulk interception and mandatory data retention) has become acutely polarised. On one side, human rights mechanisms and courts repeatedly declare its incompatibility with human rights law. On the other hand, states – if anything seemingly emboldened by the whistleblower's revelations – continue to bolster and expand their mass surveillance capabilities in the name of cybersecurity and the prevention of terrorism.

In the post-Snowden landscape, policy discourse around mass surveillance has become acutely polarised

ENCRYPTION

The most controversial – and contradictory – element of cybercrime policy relates to encryption, and its alleged role as a facilitator of cybercrime.

Law enforcement officials and government officials argue that **encryption** provides cybercriminals and terrorists with 'safe spaces' to hide from the detection of state surveillance mechanisms.

Restricting encryption and mandating the creation of state backdoors weakens security, particularly cybersecurity, rather than strengthening it. Less encryption means more online crime, as cyber criminals and identity thieves are able to navigate the insecurities in email services and banking websites with greater ease. Moreover, **backdoors** (the proposed solution to the increasing ubiquity of encryption) intended for the use of one state actor can easily be exploited by other state or non-state actors. Once a backdoor exists, it is incredibly difficult to restrict who might get in.

Despite this, some states continue to argue that encryption poses insurmountable barriers to legitimate law enforcement activity, and have called for the adoption of legislation banning encryption or mandating the installation of backdoors:

In October 2014, US FBI director James Comey warned that "encryption threatens to lead us all to a very, very dark place," and called for a debate about placing obligations on corporate entities to provide 'backdoor' access to encrypted services. The debate continues to rage in the US on this issue. State legislators in New York and California introduced bills in January 2016 banning the retail sale of smartphones with full-disk encryption. In early 2016, the FBI began proceedings against Apple in which it sought to compel the company to build a new version of the iPhone operating system, circumventing security features, and install it on an iPhone recovered during an investigation into the 2015 San Bernardino terrorist attacks.. The FBI ultimately withdrew proceedings after an 'outside party' assisted the government with breaking into the iPhone.

In June 2015, British Prime Minister David Cameron told Parliament he was intent on "ensur[ing] that terrorists do not have a safe space in which to communicate". In November 2015, the government introduced the Draft Investigatory Powers Bill, which placed numerous obligations on communications service providers to facilitate interception, and empowered the Secretary of State to place obligations on companies to remove 'electronic protections' on communications.

However, there are some positive developments in this area too, as the recognition that weakening **encryption** (a tool for the achievement of cybersecurity) in the name of cybersecurity, is likely to lead to a deterioration of security, not to mention human rights protections:

- In June 2015, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, released a landmark report which noted that encryption and anonymity create a 'zone of privacy' which is essential to the enjoyment of the rights to freedom of opinion and expression.
- In September 2015, the Indian government introduced a draft policy which would have seen encryption nullified by requiring Indians to store plain-text versions of their encrypted data for 90 days and make it available to security agencies. The policy was withdrawn following the public outrage that followed its publication.
- In January 2016, the French government rejected a proposed bill that would have required equipment manufacturers to consider the needs of law enforcement and intelligence authorities when designing technologies, inserting backdoors into devices.
- In a letter published in January 2016, the Dutch Ministry of Security and Justice said that any moves to weaken or backdoor encryption "would have undesirable consequences for the security of information stored and communicated and the integrity of ICT systems, which are increasingly of importance for the functioning of society."

HAVEN'T WE BEEN HERE BEFORE? THE CRYPTO WARS

Debates on restricting encryption are nothing new. In the 1990s, the world witnessed the first 'Crypto Wars', which pitted the US government against the technology sector. In the 1970s, the US government classified encryption algorithms as a munition for the purpose of export controls, meaning that encryption developed in the US could not be shared beyond its borders. At the time, encryption products were mostly being used in the military, rather than civilian, field.

Fast forward to the 1990s, when mass market encryption products such as Pretty-Good-Privacy (PGP) were being made available to the public, and the US government sought to enforce the controls on encryption developers. They also attempted to prosecute the developer of PGP, Phil Zimmerman. Technologists and activists reacted by printing encryption ciphers and keys on t-shirts and in hard copy when travelling abroad as a protest against the US' application of the controls.

Around the same time, encryption was being rolled out in digital telecommunications networks. In response, the Clinton administration attempted to get the technology industry to adopt an encryption backdoor scheme called the 'Clipper Chip', a physical encryption device that network operators would place on their networks, for which the government would possess a decryption key. When that scheme was rejected by the industry, the US government pressed for other forms of **key escrow**, and encouraged other countries, including the UK, to propose similar schemes. However, industry opposition, including from the banking industry, civil society outrage, and a change of administration following the US elections in 2000, saw attempts at key escrow abandoned.

Export controls on cryptography remain in place in many countries, but are rarely enforced against commercial encryption products and services.

The protection and promotion of encryption is critical, not only for ensuring robust cybersecurity, but to the enjoyment of human rights in a private space where opinions and ideas can be freely shared. It is only by securing communications against outside interference that ordinary internet users, human rights defenders, opposition politicians, dissidents and political activists, and investigative journalists can operate securely. Furthermore, there is a human rights imperative for mass – as opposed to selective - adoption of encryption. At present, individuals using encrypted communications security tools may – ironically - mark themselves out for additional scrutiny by the state. Generalised usage of encryption would avoid this.

ANONYMOUS INTERNET USE

Whereas encryption provides security from interference with the content of a communication, it does not guarantee the anonymity of the sender or recipient of that communication, and separate measures must be taken to mask one's identity from detection. These measures may range from the use of a pen name or pseudonym, to the use of non-registered SIM cards and the use of anonymisation tools such as onion routers. Given the nature of data analysis tools, multiple layers of anonymity may be needed to genuinely protect an individual from being identified, particularly when using digital tools and platforms when communicating. Remaining anonymous is a means of exercising one's privacy, and it may also be a means or precursor to freely expressing oneself, particularly where the expression of controversial opinions, beliefs or affiliations may challenge the status quo and place the person expressing them in danger or at risk of other rights violations.

THE DEEP WEB, THE DARK NET AND TOR

With pervasive corporate and government data collection, it is increasingly difficult to maintain anonymity online. Even the use of encryption does not provide anonymity, and using pseudonyms is unlikely to provide complete anonymity, particularly when using internet or mobile service in a country with mandatory data retention or SIM card registration.

The internet was never supposed to be a governed and indexed space, yet parts of it have increasingly become like that. Nevertheless, there are other parts of the internet which aren't indexed and organised: the 'deep web' refers to all of the web pages that search engines cannot find. These include databases, webmail pages and pages behind paywalls.

Existing in the deep web are a collection of websites that are publicly visible, but which hide the IP addresses of the servers that run them. Anyone can visit them, but you cannot find them with search engines. And it is difficult to find out who runs them, because the owner's identity is usually hidden using the Tor encryption tool, or similar services such as I2P. This collection of websites is sometimes called the 'dark net', with the implication and presumption being that it hosts mainly illegal activity.

To access a 'dark net' site, the user needs to be using the same encryption tool as the site, usually a Tor browser. However, individuals can and do use the Tor browser for normal browsing activities; Tor functions to conceal a user's location and usage, and makes it difficult for internet activity to be traced back to the user. Tor is used by human rights defenders, journalists and activists around the world.

Anonymity and the rights it protects are threatened by a range of measures purportedly designed to address cybercrime. These may include laws requiring the use of real names by bloggers and internet commentators, the registration of SIM cards and IP addresses, the production of identification at cybercafes, and the prohibition of Virtual Private Networks (see pages 26-27 for a discussion of how these measures can threaten human rights).

Anonymisation software, particularly the Tor browser, is especially under threat as law enforcement and intelligence agencies around the world try to overcome the obstacles to policing serious and organised crime on 'the dark web'. Although for the most part policy discussions recognise the 'dual-use' nature of Tor – that it is a critical tool for human rights defenders and journalists as it is also the home to Silk Road-type marketplaces for stolen and illicit goods – cybercrime policy is increasingly focused on infiltrating the network. In November 2015, the UK's intelligence agency (GCHQ) and the US equivalent, the National Security Agency (NSA) announced the establishment of a Joint Operations Cell to tackle online child exploitation on the hidden services of the Tor network, "committed to ensuring no part of the internet, including the dark web, can be used with impunity by criminals to conduct their illegal acts."

Although this is a legitimate endeavour, the techniques utilised by intelligence agencies in this domain may in fact have the impact of undermining cybersecurity. For example, these techniques include:

- The use of **malware** or computer network exploitation activities by government agencies. This relies on the stockpiling and manipulation of system **vulnerabilities** – weaknesses in software or hardware – which should otherwise be disclosed to the manufacturers of such software or hardware so they can patch the vulnerabilities. As long as governments keep the knowledge of these weaknesses to themselves, in order to use them as possible offensive tools, the software or hardware remains insecure to attack by other parties. There is a growing

movement in favour of imposing obligations on governments to disclose, rather than stockpile, **vulnerabilities** in order to support cybersecurity objectives.

- The use of fake security updates to install **malware** on a device or programme that might be used for surveillance purposes. This undermines trust in security updates and deters users from downloading them.

The appetite of intelligence agencies for ever more intrusive surveillance tools continues to grow. Documents from the Snowden archives revealed just how far US and UK intelligence agencies have gone in developing intrusion software, using malware, targeting system administrators to hack into whole companies and networks. For example, the UK recently established a National Cyber Crime Unit within its National Crime Agency, a law enforcement, not intelligence, agency. It intends to design its own intrusion software, and launch a recruitment drive to find coders to design Trojans, a type of malware designed to provide unauthorised, remote access to a user's device. A leak of corporate documents from malware manufacturer Hacking Team in July 2015 shows that countries such as Azerbaijan, Kazakhstan, Uzbekistan, Russia, Bahrain, Saudi Arabia and the UAE have all purchased **hacking** tools for use in intelligence gathering.

Like encryption bans, such activities would seem to only exacerbate cyber insecurities, rather than contribute to greater cybersecurity through gains in policing and detecting cybercrime.

INTERNET RESTRICTIONS AND SHUTDOWNS

As free and secure access to the internet increasingly becomes a prerequisite to the enjoyment of a range of human rights, from the right to freedom of expression to the right to an education, restrictions on internet functionality can have dire effects for human rights. Yet there is an increasing tendency, as shown below, for governments to order the limitation, throttling, or shutting down of the internet, or the prohibition of certain sites or services. Often, internet shutdowns are justified by reference to national security and cybersecurity concerns, and take place in the context of political events, elections and demonstrations.

Some prominent examples of internet shutdowns include:

- Around the February 2016 Ugandan presidential and parliamentary elections, the Ugandan Communications Commission ordered a three-day internet shutdown, requiring mobile service providers such as MTN Uganda to block users' access to social media sites and mobile money transfers.
- During the January 2011 protests in Tahrir Square, the Egyptian government ordered the shutdown of the internet in Egypt.
- In the aftermath of the March 2016 terrorist attacks in Ankara, the Turkish government imposed a total media blackout, and banned reporting on the "internet and social media," as well as imposing Internet Service Provider-level throttling to deny any access to coverage of the attack. The government had previously issued a blanket ban of Twitter usage in the country.
- During the Estonian cyber-attacks in 2007, the government took measures to block all international web traffic in order to cease the wave of **DDoS** or denial-of-service attacks on government servers.

- 2015 alone saw reports of shutdowns in the Democratic Republic of the Congo, Burundi, India, Bangladesh, Brazil and Pakistan.

Restrictions on the functioning of the internet and its use in the name of cybersecurity have far reaching implications for human rights. They not only prevent people from sharing and accessing information, but they impede enjoyment of those human rights which rely on the internet, from freedom of movement and association, to political participation.

Restrictions on the functioning of the internet and its use in the name of cybersecurity have far reaching implications for human rights

RECOMMENDATIONS FOR HUMAN RIGHTS DEFENDERS

Unlike the information security policy space, human rights are already present in cybercrime discourse. However, the trend so far is for human rights to receive only lip-service, or to be used as an 'either/or' intrusion into other rights – for example, when the rights of children to be free from exploitation and abuse are used to justify the implementation of blocking and filtering systems.

These are some recommendations for bringing human rights to cybercrime policy in a way that is meaningful and appropriately balances competing human rights considerations:

1. Scrutinise cybercrime legislation and advocate for the removal of provisions that regulate the dissemination of human rights-compliant content online.

Proposed cybercrime legislation often evades the scrutiny of human rights defenders because it is perceived to be too technical or specific. However, there are resources available for human rights defenders to scrutinise cybercrime legislation and assess whether it unduly interferes with human rights such as privacy. For example, the free expression organisation ARTICLE 19 has conducted many analyses of cybercrime legislation from these angles. The Council of Europe also provides a guide to human rights for internet users. It is important to understand the sources used to draft cybercrime legislation. Where a 'model law' may have been used, analysis of the model law (see Selected Resources) and knowledge of its shortcomings in relation to international best practice and law can inform effective advocacy.

2. Campaign against the use of 'cybercrime' as a means of criminalising activism and undermining the freedom of the internet.

Human rights defenders must stand up to those who misuse the threat of cybercrime, or the importance of cybersecurity, in order to crack down on legitimate speech, activism and expression online.

3. Campaign for governments to provide evidence-based justifications for any new surveillance powers.

In the aftermath of the Snowden revelations, court cases and public inquiries have led to greater transparency around surveillance techniques, declassification of secret court judgements, and the avowal of certain powers by governments who had long denied having them. These developments demonstrate that governments can be more transparent about their surveillance capabilities without undermining the effectiveness of those capabilities. The public must be encouraged

to call for greater accountability of police and intelligence agencies when it comes to surveillance, rather than accepting references to terrorism or cybercrime as justifications for intrusions into privacy.

4. Advocate against mass surveillance programmes that facilitate blanket, indiscriminate intrusions into the rights to privacy and freedom of expression.

State practice when it comes to mass surveillance is increasingly remote from the standards pronounced by regional and international human rights mechanisms. The fight against the legitimacy and legality of blanket, indiscriminate surveillance continues, and human rights defenders must weigh in – by demanding governments bring surveillance in line with human rights standards, and educating the public on the implications of mass surveillance.

5. Campaign for more research funds and long-term, sustainable financial support for human rights defenders to participate in cybersecurity debates.

Campaigns concerning the resources allocated to cybersecurity could also focus on the need to fund critical security audits for major free software building blocks like Linux, OpenSSL, and OpenOffice - software which is often built and maintained by very few people who are often working on a voluntary basis.

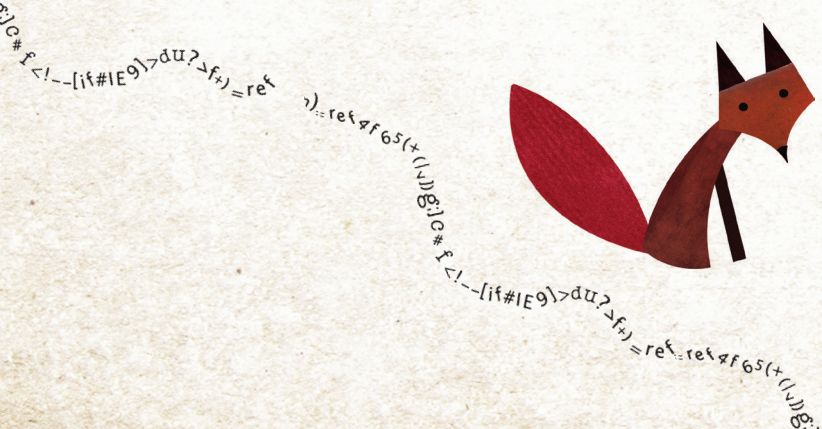
6. Call on governments to commit to supporting and protecting encryption as an essential tool of cybersecurity and a precondition for the enjoyment of human rights.

Human rights defenders should equip themselves with the tools and arguments to call out proposed bans on encryption as ineffective, counter-productive, and dangerous for cybersecurity. Advocacy in support of the companies that build and deploy encrypted tools and services may also be an effective means of shoring up support for encryption. It is essential that the public, too, understands that encryption is a tool for cybersecurity, not a tool opposed to cybersecurity.

7. Campaign against restrictions on the internet, including restrictions on anonymity.

Online **anonymity** should not be viewed as a thing of the past, or a lost cause. It is an essential component of the right to freedom of expression, and something worth fighting for. Companies must be educated about the problematic implications of real name policies, and encouraged to allow their users to make use of pseudonyms. Laws which require mandatory registration of SIM cards should be critiqued both on privacy grounds and for the ineffectiveness of this measure in preventing and detecting crime.

Human rights defenders should push back against government efforts to eradicate anonymisation software such as the Tor browser, and point to the essential role played by the Tor network in enabling human rights defenders themselves to communicate securely.



CHAPTER IV

CYBERSECURITY AS CYBER CONFLICT

Cybersecurity As Cyber Conflict

The area of cybersecurity policymaking which attracts the most public attention is the least mature policy area - the question of what laws and norms should regulate the way government relate to each other in cyberspace. Or, to put it more simply: what are the rules that states have to play by?

MAJOR POLICY PRIORITIES AND DEBATES

Ordinary people (read: those who aren't international law geeks) might be surprised to discover the high degree of agreement between governments on the rules of international relations and security: the conditions under which the use of force by one state against another is justified, and the terms on which conflict should be conducted. Such issues are regulated by the United Nations Charter and the variety of treaties and customary law which comprise international humanitarian law. Even if governments don't always play by these rules, they still acknowledge and endorse them, even if hypocritically. When it comes to offline conflict, states are far more likely to justify blatant contraventions of the rules as exceptions ("the rules don't apply here because…") rather than through outright rejection ("there are no rules…").

But ever since the emergence of the prospect of 'cyberwar', and its numerous variations and precursors such as **cyber-attacks**, cyber espionage, cyber operations, and cyber vandalism, debate has raged about what, if any, rules apply to international conflict in cyberspace. The unsettled issues include:

- What constitutes a cyber-attack?
- Under what circumstances can a state take action to preempt a cyber-attack?
- To what level must a cyber operation rise in order to constitute a cyber-attack equivalent to a 'use of force' under the UN Charter?
- Can states legitimately respond to a cyber-attack with a use of force in the offline world?
- Should states refrain from attacking each other's critical infrastructure in peacetime? How about during an actual armed conflict?
- What is a cyber weapon, and how can it legitimately be deployed?
- What is the appropriate way to regulate the use of autonomous weapons systems?

An overarching question is what role does international human rights law play with respect to norms in cyberspace? The Tallinn Manual (see page 88), an academic soft-law initiative, argues for the application of international humanitarian law to questions of cyber conflict. The creation of the Manual was funded by the North-Atlantic Treaty Organisation (NATO), although member states were not consulted and it took place behind closed doors, with no opportunity for human rights voices to be heard. As a result, the set of laws and norms it elaborates differs considerably from human rights law, and arguably provides a lower level of protection for individuals.

For example, the concept of proportionality under international humanitarian law is far more malleable than in human rights. It is not concerned with the impact of a particular measure (like a bombing) on the enjoyment of human rights of all individuals (such as enemy combatants), but only with the collateral damage on civilians. Proportionality under human rights law is much more demanding.

THE TALLINN MANUAL

The Tallinn Manual on the International Law Applicable to Cyber Warfare, and its successor publication, due for publication in 2016, is an academic initiative convened by the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE). The manual, authored by a group of twenty international experts and published in April 2013, seeks to identify 'black letter' rules of international law relevant in the cyber context. Black letter rules refer to law that is written in treaties and texts, rather than law that is developed through jurisprudence, custom or practice. They also provide commentary on the application of those rules.

While the focus of the original manual was the most disruptive cyber operations – those which rise to the level of 'armed attacks' when existing international law of war is applied by analogy – the subsequent publication will address cyber operations which don't rise to such a threshold, and provide guidance as to the applicable legal regimes.

The original Tallinn manual has been subject to substantial analysis and critique (see, for example, Thomas Rid's "Cyber War Will Not Take Place" in Selected Resources). At a very basic level, the manual certainly contributes to the securitisation of the discourse around cybersecurity (see page 28) and risks encouraging the escalation of debates on activities in cyberspace to the level of conflict. Civil society has expressed legitimate concern that the second manual, which deals with 'cyber operations', could also have a harmful impact if it encourages the application of international humanitarian law, rather than international human rights law, to activities in cyberspace which don't rise to the level of attacks. Although the Tallinn Manual is an academic work, which was not subject to a multistakeholder development process, and includes no input or comment from civil society, it is often quoted as an authoritative source in policy processes concerning norm development around cyber conflict.

There is a risk that if the debate around the norms applicable to cyber conflict excludes the voices of human rights experts and advocates, and focuses primarily on the comparatively lax framework of international humanitarian law, human rights will be seriously disadvantaged. There is some existing human rights advocacy in this space. For example, in 2015 a group of organisations including Article 36, the International Committee for Robot Arms Control, and the Just Net Coalition (JNC) submitted a statement to the United Nations General Assembly First Committee on Cyber, Disarmament and Human Security, calling for norms of cyber conflict to reflect the following guidelines:

- The existing legal framework, including human rights law, applies to cyberspace. At the same time, it should not be seen as sufficient, and states will need to go beyond a reiteration of existing, general rules, recognising that cyberspace needs to be addressed in its own terms.
- The internet should remain civilian infrastructure, and should not be made the target or the medium for attacks.
- States should establish the strongest norms against such attacks, and not drift into an acceptance or legitimation of established practice.
- Norms should promote an internet that is used for peaceful purposes, and resist the current drift toward normalising offensive capabilities.

In some aspects such guidelines are controversial, as they may feed into the narrative of the exceptionalism of cyberspace which some argue contributes to sidelining traditional human rights considerations.

Unlike the previous two cyber policy areas discussed here, many of the discussion concerning norms are still happening on a bilateral basis, and there are very few policy forums where cyber conflict is being formally discussed.

RELEVANT POLICY FORUMS

THE UN GENERAL ASSEMBLY

The First Committee of the General Assembly, which focuses on disarmament and international security, has been considering questions of cyber conflict since Russia introduced a draft resolution in the Committee in 1998.

In 2004, the Committee convened its first Group of Governmental Experts (GGE) to examine the threats posed by the 'cyber-sphere' and possible cooperative measures to address them. Two substantive disagreements emerged amongst the group: first, the degree to which the impact of cyber issues on national security and military affairs should be emphasised in the report; and second, whether the issue of information security related only to information infrastructure, or extended to insecurities caused by the content of information itself.

Although the 2010 GGE issued a successful report which reached consensus on, among other things, the need for dialogue among states on norms in cyberspace and the need to protect critical infrastructure, in 2011 the issue of insecurities caused by information content came up again. That year, China, Russia, Tajikistan and Uzbekistan proposed a draft resolution on an international code of conduct for information security and called for international deliberations within the UN framework on such a code. The draft resolution adopted a definition of 'information security' which exceeded in scope the narrower, technical definition discussed in this guide by referencing the ability of information itself to cause insecurity (see page 36).

The 2013 GGE report reached agreement on a number of substantive issues related to norm development, critically - and for the first time - agreeing that existing international law applies to cyberspace. The report affirmed:

- International law, in particular the UN Charter, is applicable to the cyber-sphere and is essential for an open, secure, peaceful and accessible ICT environment.
- State sovereignty applies to states' conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.
- State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms.
- States must not use proxies to commit internationally wrongful acts and must ensure that their territories are not used by non-state actors for unlawful use of ICTs.
- The UN should play an important role in promoting dialogue among member states.

These findings were further developed, without substantive alteration, in the 2015 report. It was also recommended, for example, that states should not conduct cyber activity "that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public," and should not knowingly support activity that harms information systems of authorised emergency response teams (such as **CERT**s) or use CERTs to engage in malicious international activity.

Questions remain as to the meaning of the GGE's agreement and the unresolved issues which were not addressed in the report; namely, *how* does international law apply to cyberspace? That agreement was not reached on these more substantive issues suggests that norm development is still plagued by the divergent positions of the major states engaging in it.

A further GGE will convene in 2017. However, some have suggested that any remaining room for consensus, particularly with regards to the application of international law, has been exhausted. Moreover, the GGE is made up of only 20 states, ten percent of UN members.

Building the legitimacy of cyber norms will ultimately require the buy-in of the UN membership as a whole at a level beyond mere rhetoric, with additional input from technical experts and civil society.

THE LONDON PROCESS AND THE GLOBAL CONFERENCE ON CYBERSPACE (GCCS)

The GCCS was inaugurated in 2011, when the UK and the Netherlands convened a high-level discussion on cybersecurity, cybercrime and the norms applicable to cyberspace in London. Since that time, the GCCS has convened in Budapest (2012), Seoul (2013), and The Hague (2015). It aims to provide a multistakeholder environment for the discussion of cybersecurity and the norms of cyber conflict, and the transference of capacity on cybersecurity issues.

THE UN SECURITY COUNCIL COUNTER-TERRORISM COMMITTEE (CTC)

The CTC has responsibility for monitoring compliance with Resolution 1373 (2001), passed in the aftermath of the September 2001 terrorist attacks, as well as Resolutions 1624 (2005) and 2178 (2004) which require states to criminalise, prosecute and investigate terrorist activities, the funding of terrorist activities, and foreign terrorist fighters.

Although the CTC doesn't have a direct mandate to tackle cyber conflict and security issues, it has begun to look at cybercrime and cybersecurity issues as they pertain to terrorists' use of

the internet and social media. In particular, the CTC intends to continue to assess states' implementation of the above named resolutions, particularly as they apply to the internet and digital technologies – focusing on strengthening cooperation in preventing the use of ICT for terrorist purposes, and taking measures against incitement to violence online.

FREEDOM ONLINE COALITION WORKING GROUP I

Established in 2011, the Freedom Online Coalition had 29 member states (as of 2015) across the Americas, Asia, Africa, Europe and the Middle East, all of whom have committed to the principle that human rights apply online as they apply offline. The Coalition coordinates diplomatic efforts regarding internet issues, and provides a platform for multistakeholder engagement, including through the yearly Freedom Online Conference.

The FOC has convened three multi-stakeholder working groups which work continuously throughout the year to develop thinking and engagement on key internet freedom issues. Working Group 1 focuses on 'An Internet Free and Secure', and aspires to – among other things – advance the normative debate on cybersecurity, including by developing a set of recommendations that promote stakeholder-driven and human rights respecting approaches to cybersecurity.

THE GLOBAL COOPERATION IN CYBERSPACE INITIATIVE

Founded and operated by the EastWest Institute, an independent non-profit organisation, the Initiative aims to create a multi-stakeholder space to bring together disparate actors to solve problems around cooperation and conflict in cyberspace. The Initiative convenes summits, produces working papers and, most importantly, discreetly brings together actors that would otherwise not necessarily be at the same table to discuss the developments of norms in this space.

RECOMMENDATIONS FOR HUMAN RIGHTS DEFENDERS

Cyber conflict policymaking is the least developed area of cybersecurity policymaking and largely takes place in multilateral forums which are traditionally not very open to civil society. However, these are some recommendations for ways in which civil society can advocate with states to bring human rights to the table:

1. Advocate with member states of the GGE to ensure human rights considerations are at the top of the GGE's agenda.

The GGE continues to be the main forum in which cyber conflict norms are openly discussed and debated. The members of the GGE need to be made aware of the human rights implications of their work through advocacy and education.

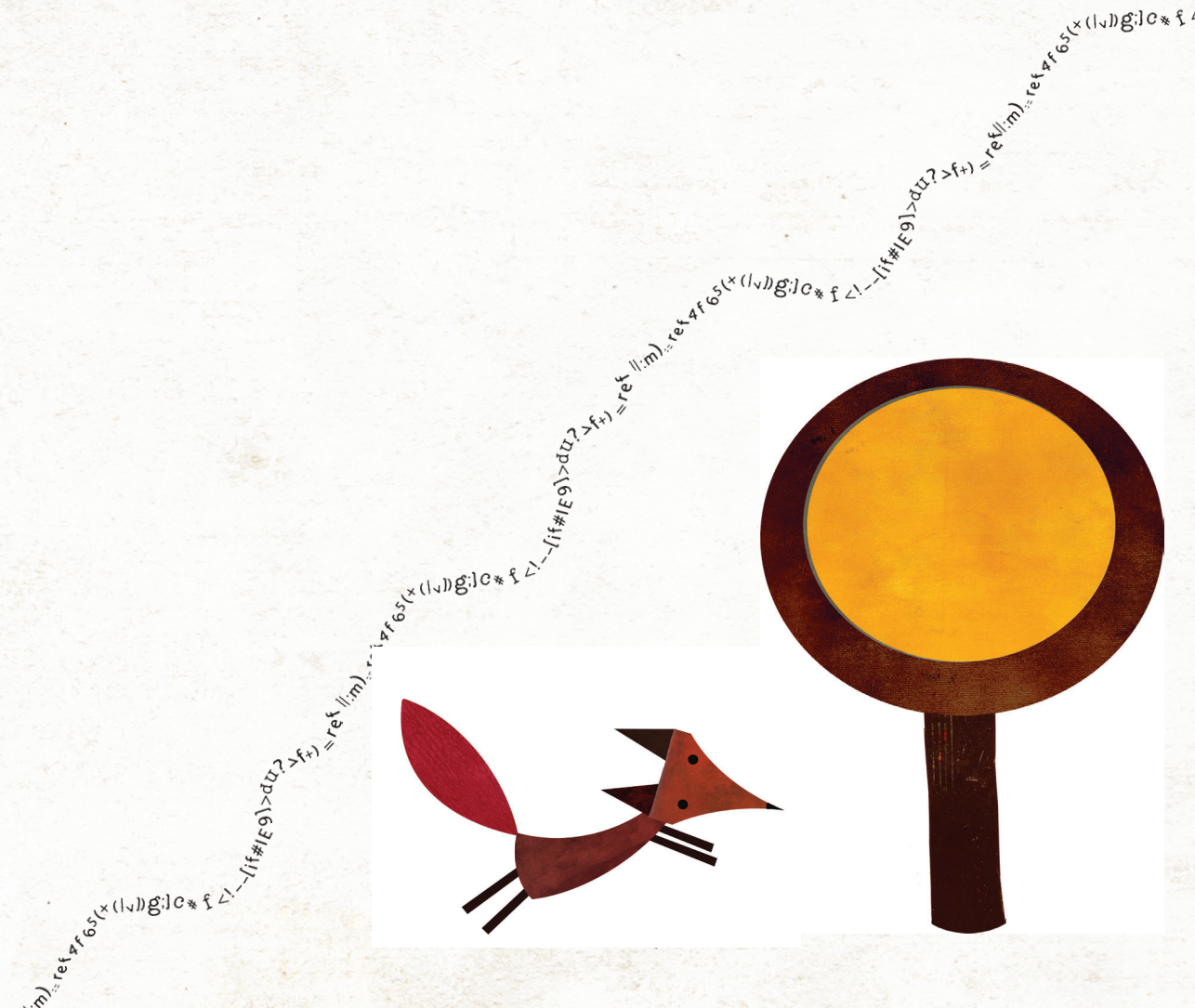
2. Engage with the First Committee on Disarmament at the annual General Assembly sessions.

Human rights organisations, led by Article 36, are already engaging in the First Committee by presenting a statement on cyber issues each year in the annual General Assembly sessions. Increasing the scope of human rights defenders' engagement with the First Committee will reiterate to states the importance of this issue, and reinforce pressure to ensure human rights remain central to debates on security and conflict.

3. Engage in multistakeholder processes and promote the use of human rights language and standards in all debates about cyber conflict.

It is essential that civil society is in the room when decisions about the norms of cyberspace are being made. Just showing up to multistakeholder events like the GCCS (see page 92) demonstrates to states and the private sector that these issues are of critical importance to human rights defenders, and

ensures that human rights remain on the agenda. Equally, the release of the second Tallinn Manual and other academic and soft-law initiatives should be met with engagement and, where justified, criticism from civil society, in order to ensure that proposed norms aren't accepted or entrenched in the absence of rigorous debate.



PRINCIPLES FOR CYBERSECURITY POLICY ENGAGEMENT

The strategies and opportunities for bringing human rights to information security, cybercrime and cyber conflict policymaking advanced in this guide are only a suggested starting point for human rights defenders' engagement with the field of cybersecurity. There are many more ways in which human rights can be placed at the centre of cybersecurity policy, and each organisation will have a different approach. A study commissioned by Mozilla developed a list of 36 policy recommendations (see Selected Resources) that might also provide inspiration to human rights defenders considering entering this policy space.

To conclude, this section outlines some best practice principles for engagement with cybersecurity policy that human rights defenders should attempt to adopt and integrate into their work.

1. Take control of the language.

As this guide has consistently reiterated, the language of cybersecurity is often used to militarise or securitise a debate that can otherwise be framed in terms of human rights and responsibilities. Controlling the language used can impact on the direction of a particular policy debate. It is essential that human rights defenders emphasise at every point that cybersecurity issues are human rights issues - no matter which angle you view them from.

2. Move the debate from trade-offs to reinforcing rights.

Too often debates around cyber policy present security and human rights as locked in a zero-sum game; that to gain one, we need to forfeit the other. Human rights defenders can play a critical role in educating policymakers and stakeholders about the interdependent and reinforcing nature of human rights and cybersecurity, and demonstrate how security can co-exist with the enjoyment of rights to privacy and freedom of expression.

3. Meet opinions with facts.

Engaging credibly in cyber policymaking spaces requires investment in building individual and organisational capacity, knowledge and expertise on the technical and legal issues underpinning the cybersecurity policy space. Human rights defenders need to become comfortable with technical subjects and emerging areas of law to ensure they are given an equal seat at the policymaking table.

4. Support and engage with multistakeholder initiatives.

The nature of cybersecurity, and its associated threats and opportunities, demands the involvement of stakeholders from a broad range of sectors and disciplines. This is not an issue which can, or should, be resolved through state policymaking alone; the private sector, technical and academic communities, and civil society all have a critical role to play in devising, validating and implementing cybersecurity policy.

The involvement of non-state actors in the policymaking process can provide important insurance against discourses becoming dominated by governmental interests, and may diminish the likelihood that human rights concerns will be ignored.

5. Use existing soft-law standards to reinforce messaging.

Human rights defenders have a number of key advocacy tools at their fingertips, including soft-law standards such as the International Principles on the Application of Human Rights to Communications Surveillance (the Necessary and Proportionate Principles), and the Global Principles on National Security and the Right to Information (the Tshwane Principles). Both are human rights instruments which enjoy broad support from a range of civil society organisations and experts, and provide guidance on how human rights should be applied to questions of technology and the internet.

6. Lead by example.

Make use of the technical tools available to advance cybersecurity, including encryption and anonymisation tools and open source software. Doing so may both incentivise those who make and build such tools to continue investing in them, and also gain government and public buy-in for their use.

GLOSSARY

Anonymity – the condition of avoiding identification. Encryption does not provide anonymity: whereas encryption tools ensure that the content of a communication are indecipherable by no one but the intended recipient, they don't provide either the recipient or the sender with anonymity. When parties use encryption, the **metadata** associated with a communication are not encrypted. Should an individual wish to remain anonymous, they need to use anonymisation tools and methods, such as using pseudonyms or anonymisation tools such as Tor.

Backdoors or 'backdooring' – a colloquial term used to refer to measures that weaken or undermine encrypted tools, devices and services in order to facilitate unauthorised access to information and communications by actors other than the creators of, and parties to, the information or communications. There are many ways to 'backdoor' a system or device; such measures may include state measures compelling the providers and engineers of encryption tools and services to:

- Generate and retain encryption keys to accommodate the eventuality of government access to information and communications;
- Hold encryption keys in escrow so that, under certain circumstances, an authorised third party may gain access to those keys to perform decryption (known as '**key escrow**');
- Diminish the strength of encryption used in encrypted tools, devices and services; or
- Deploy only approved forms of encryption or specific state-approved random number generators.

Another form of backdoor which has recently gained attention are measures to compel companies to generate and deploy software updates that would diminish or remove the encryption from a particular device, tool or service. Although this is called a backdoor, it might also be described as an attempt to circumvent encryption in order to gain unauthorised access to information and communications, which is generally called **hacking**, computer network exploitation or equipment interference.

Botnet – a number of internet-connected computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the internet.

Cyber-attack – a term generally used to describe the use of a computer to gain unauthorised access, cause damage to or destroy information, devices, systems or networks.

CERT – Computer Emergency Response Team. Most countries maintain a national CERT responsible for responding to national cybersecurity incidents, and supporting companies which maintain critical infrastructure to respond to cybersecurity incidents.

CSIRT – Computer Security Incident Response Team, a term which is interchangeable with CERT (above).

DDoS attack – a distributed denial-of-service (DDoS) attack occurs when multiple computer systems flood the bandwidth or resources of a targeted system. Such an attack is often the result of multiple compromised systems (for example a **botnet**) flooding the targeted system with traffic.

Encryption – a mathematical process of converting messages, information, or data into a form unreadable by anyone except the intended recipient. Most of us encounter one of three different types of encryption in our daily internet usage:

- **End-to-end encryption** is when the keys to decrypt communications are held exclusively by the sender and recipient of the communication. When end-to-end encryption is deployed, any intermediate device or service provider with access to your electronic communications, or any entity attempting to intercept the communications, is unable to read their contents. For example, anyone who intercepts end-to-end encrypted iMessages or WhatsApp messages cannot read them.
- **Disk or device encryption** is the process by which all of the information stored in computers or smartphones is encrypted when residing on the device. With device encryption, the data on a device will not be able to be read or accessed by anyone who doesn't have the PIN or password to the device, including the company which manufactured the device or its software.
- **Transport encryption** is the practice of encrypting information and data as it traverses a computer network. Types of transport layer encryption include HTTPS, Secure Socket Layer (SSL) and Transport Layer Security (TLS). These types of encryption, in effect, encrypt individuals' interactions with particular websites accessed through their web browser. When a website operator has the data, it is in an unencrypted format. This means that it can be disclosed to law enforcement or accessed in intelligible form only once it reaches the target company or website.

Going dark – a phrase used by US law enforcement (and appropriated by others) to describe the declining capabilities of law enforcement agencies to access the content of communications due to the increased use of encryption in everyday technologies and services. It is important to note that encryption generally will not prevent interception of

communications, nor does it render communications completely void of any intelligence information. Intercepting authorities will still be able to derive some information (such as a date, time, senders, size etc.) from the intercepted encrypted communication.

Hack or hacking – unauthorised access to an application, system or network. Also known as computer network exploitation, intrusion, equipment interference, remote access and remote search.

Key escrow – refers to an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorised third party may authorised access to those keys and subsequently to the data they protect.

Malware – malicious software that goes against the intentions of the computer user, often to provide remote access and disclose information to unauthorised entrants. Malware will often be covert, disguised as something else (a feature that earns it the name 'trojan') and will be designed to avoid detection and analysis. Malware will often allow an attacker to control functions of the device or application, such as remotely turning on the microphone or webcam.

Mass surveillance – a term used to describe the blanket, indiscriminate monitoring of people or their private information, without suspicion of any wrongdoing or attempt to target particular people or data. In recent years, it has come be used in conjunction with the 'bulk interception' of communications content and metadata.

Metadata – refers to all information that is generated through the use of communications technology other than the actual content of the communication. While the information does not necessarily contain personal or content details, it contains information about the devices being used, the users of the devices, and the manner in which they are being used.

Ransomware – a type of malware that restricts access to the infected computer or device in some way, and demands that the user pay a ransom to the malware operators to remove the restriction.

Vulnerabilities – security flaws or weaknesses in software and hardware that are regularly identified and fixed ('patched') by designers and manufacturers.

Zero-day vulnerabilities – When a vulnerability is not disclosed to the software manufacturer, but rather used by offensive actors, it is called a 'zero-day' vulnerability. Zero-day vulnerabilities can often be exploited immediately.

SELECTED RESOURCES

The Berkman Centre for Internet and Society, 'Don't Panic. Making Progress on the Going Dark Debate,' (2016) available at https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

Centre for the Democratic Control of the Armed Forces, 'Democratic Governance Challenges of Cyber Security' (2010) available at http://www.dcaf.ch/Publications/Democratic-Governance-Challenges-of-Cyber-Security

Farrell H., 'Promoting Norms for Cyberspace,' *Council on Foreign Relations*, (2015) available at http://www.cfr.org/cybersecurity/promoting-norms-cyberspace/p36358?cid=otr-marketing_use-norms_cyber_brief/

Freedom Online Coalition, 'Mapping Cybersecurity: A visual overview of relevant global spaces in 2015' (2015) available at http://www.gp-digital.org/wp-content/uploads/2015/07/Mapping-Cybersecurity-----A-Visual-Overview-Of-Relevant-Global-Spaces-In-2015.pdf

Green, N. and Rossini, C. 'Cyber Security and Human Rights' (2015), *Public Knowledge*, available at https://www.gccs2015.com/sites/default/files/documents/Introduction%20Document%20for%20GCCS2015%20Webinar%20Series%20-%20Cybersecurity%20and%20Human%20Rights%20(1).pdf

Hawtin, D. and Kovacs, A. 'Cyber Security, Cyber Surveillance and Online Human Rights' (2012) available at http://www.gp-digital.org/wp-content/uploads/pubs/Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf

International Telecommunications Union, 'Understanding Cybercrime: Phenomena, Challenges and Legal Response' (2012) available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Jamil, Z. (2014) 'Cybercrime model laws: draft Discussion paper prepared for the Cybercrime Convention Committee (T-CY)' available at https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/3021_model_law_study_v15.pdf

Jardine, E. 'The Dark Web Dilemma: Tor, Anonymity and Online Policing,' (2015) *Global Commission on Internet Governance Paper Series 21.*, available at https://www.cigionline.org/sites/default/files/no.21.pdf

Mozilla Cybersecurity Delphi 1.0: Towards a user-centric policy framework (2015) available at https://blog.mozilla.org/netpolicy/files/2015/07/Mozilla-Cybersecurity-Delphi-1.0.pdf

National Institute for Standards and Technology, 'Interagency Report on Strategic US Government Engagement in International Standardisation to Achieve US Objectives for Cybersecurity' (2015) available at http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v1.pdf

Osula, A.M 'Accessing Extraterritorially Located Data: Options for States,' (2015) *NATO Cooperative Cyber Defence Centre of Excellence* available at https://ccdcoe.org/sites/default/files/multimedia/pdf/Accessing%20extraterritorially%20located%20data%20options%20for%20States_Anna-Maria_Osula.pdf

Privacy International 'Eyes Wide Open' (2013) available at https://www.privacyinternational.org/sites/default/files/Eyes%20Wide%20Open%20v1.pdf

Rid, T., (2012) 'Cyber War Will Not Take Place'

The White House 'International Strategy for Cyberspace' (2011) available at https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

ACKNOWLEDGEMENTS

This guide was drafted by Carly Nyst, and edited by the brilliant staff of Global Partners Digital. Special thanks go to Sheetal Kumar for shepherding the guide from inception to publication. Additional assistance, feedback and input was gratefully received from Camille Francois, Anita Gohdes, Aaron Martin and Eric King.

Produced by The Kitchen agency
Designed by Miriam Hempel | Illustrations by Valentina Cavallini

GLOBAL PARTNERS DIGITAL

The rapid digitisation of human life has made cybersecurity a key priority for policymakers worldwide. In a context marked by contested definitions of what cybersecurity is and how it should be achieved, it is critical for human rights defenders to understand the situation, actors and issues at stake in order to engage meaningfully in these debates.

Depending on who you talk to, and where, cybersecurity can extend to issues as diverse as security protocols in government databases to the international norms applicable to cyber-attacks during armed conflict.

Engagement by human rights defenders in cybersecurity policy is important for a number of reasons, not least because the term has been appropriated for a wide number of measures that can undermine human rights. This guide aims to help human rights defenders navigate this complex policy domain.

Cybersecurity Policy for Human Rights Defenders is the third entry in the Travel Guide to the Digital World series, which is designed to help newcomers understand, follow and engage in internet policy and governance debates. Find the rest of the series on the Global Partners Digital website.

ISBN 9789380765150