PRIVACY INTERNATIONAL

Giving the Tin Man a Heart

Cyber Security in the Global South

May 2017

CYBER SECURITY IN THE GLOBAL SOUTH

Giving The Tin Man A Heart

May 2017

PRIVACY INTERNATIONAL

www.privacyinternational.org

Table of Contents

Introduction	4
PART 1: What Does It Mean To Be Secure? A Privacy Focused Approach To Cyber Security	6
PART 2: Global Cyber Security Policies, Practices and Laws That Undermine Cyber Security	13
Conclusion	22

Introduction

Privacy International defends privacy world-wide. We hold government and industry to account and demand meaningful protections and safeguards. Privacy is a fundamental right, and will be increasingly essential to freedom in a data driven world. We believe that for liberty to thrive, both technology and law must secure our right to privacy.

Privacy International continues to work to build and support a global privacy movement of civil society partners who are equipped to engage in relevant debates with policy makers, national governments and regional bodies. We aim to challenge current narratives and develop new perspectives that are rights respecting and technology aware, thereby reconceptualising what it is to be secure and economically empowered in a modern society. As part of a project focused on Africa and Latin America, Privacy International and partners in the regions are developing research, advocacy strategies and policy recommendations on cyber security and privacy. The project aims to equip civil society partners with the knowledge and confidence to constructively contribute to policy processes and when necessary to challenge government approaches to cyber security.

This first paper in a series by Privacy International lays the groundwork for our work on cyber security policy in the global south. Part 1 describes what we believe "good" cyber security looks like. Part 2 sets out global examples of government policy, law and use of technology that we believe undermine cyber security, and sets out a basic set of recommendations for civil society to be advocating within policy processes. More detailed outputs with a technical and regional focus will follow as part of the project.

Cyber Security—For Whom and of What?

Describing cyber security can often feel like a riddle. It is a term widely used but poorly understood. It has no internationally accepted definition. It can mean different things to different communities, governments and companies. Nonetheless, in the name of cyber security, governments are adopting laws and policies that affect everyone.

Cyber security discussions often provoke more questions than they answer. What is cyber security to the person or institution you are engaging with? Is it the legal mechanisms to detect the theft of valuable private information, or to prevent the sale by criminals to the highest bidder? Is it the arsenal of responses to State and State-sponsored hackers reportedly wanting to influence how we vote? Or is it about preventing against shadowy forces wanting to turn off our lights and launch our missiles by attacking our core systems? Who decides what cyber security is?

It is not surprising that the public are often confused about what type of security the world needs when the threats and implications are simultaneously unclear, multiple, and diverse. Whether it is the security of their selves, devices, data, the services they use, the infrastructure their daily lives depend upon, their political systems, or their sense of security, the public is inundated with security concerns everywhere and every day.

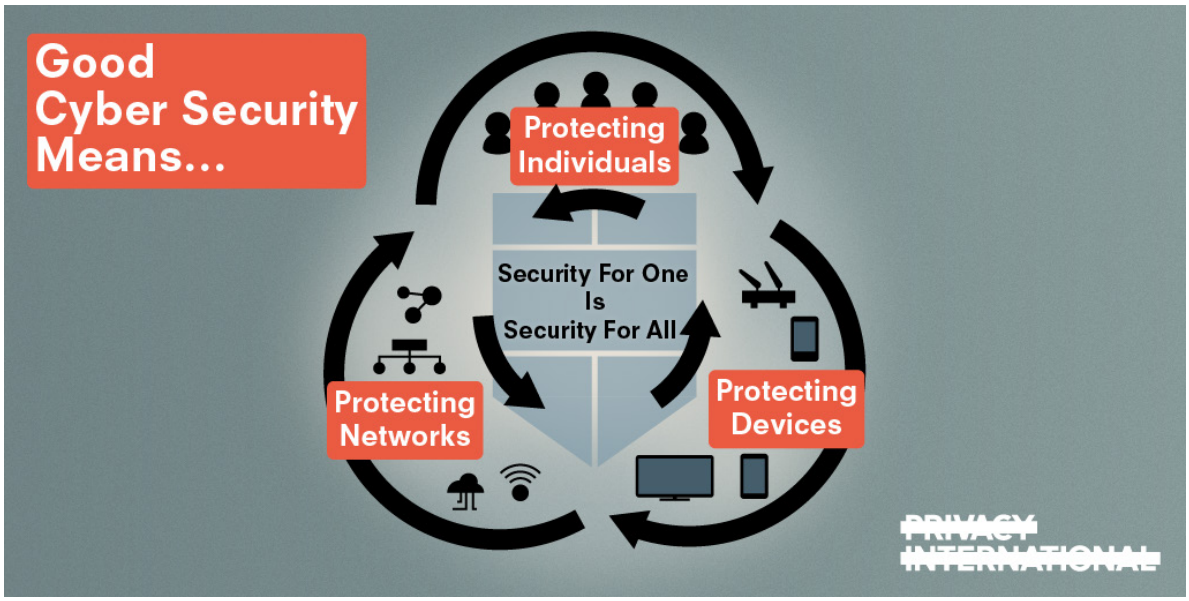
In turn, civil society organisations are also often perplexed. Those who are beginning to engage with the global cyber security debate from a human rights perspective are unclear on the best path. The dizzying scale, technical complexity and downright panic accompanying 'cyber attacks' and data breaches often overshadows and distracts from the fact that human rights should be at the heart of cyber security, just as human rights should be at the centre of all debates around all forms of security.

PART 1: What Does It Mean To Be Secure? A Privacy Focused Approach To Cyber Security

Privacy International believes that privacy and security are both essential to protecting individuals, including their autonomy and dignity.

Undermining privacy undermines the security of individuals, their devices and the broader infrastructure. People need privacy to freely secure themselves, their information, and fully enjoy other rights. In turn, the systems that constitute our modern infrastructure, whether commercial or governmental, must be secure and aid in securing privacy. Technological systems must support and enhance privacy, not undermine it. Laws or practices must not compel individuals or organisations to undermine their security or the security they provide to the users who place their trust in them.

Too often governments and companies have chosen to undermine privacy through alterations or intentional designs into common and widely-used infrastructure. Too many components of our telecommunications systems, for instance, are designed and implemented in a time when security wasn't a primary consideration, undermining the privacy and security of individuals, groups, and whole communities.[1]



[1] For example, SS7 is a system that routes messaging and calls over our cellular networks worldwide, and has vulnerabilities that can be exploited. This has led to calls from legislators for a fix. See, Sean Gallagher, Congressman to FCC: Fix phone network flaw that allows eavesdropping, Arts Technica 26 August 2017 https://arstechnica.com/security/2016/08/congressman-to-fcc-fix-phone-network-flaw-that-allows-eavesdropping/
See also, US Senator Ron Wyden press release, Wyden, Lieu Call On FCC to Address Major Security Weaknesses in Cell Phone Networks, 28 March 2017 https://www.wyden.senate.gov/news/press-releases/wyden-lieu-call-on-fcc-to-address-major-security-weaknesses-in-cell-phone-networks
And, Iain Thompson, After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts, The Register, 3 May 2017 https://www.theregister.co.uk/2017/05/03/hackers_fire_up_ss7_flaw/

As such, cyber security should be considered a public good, in the same way as public health for example, which promotes collective responsibility for the benefit of everyone.[2] In a cyber security context, securing the individual helps secures everyone. In order to secure the individual, the priorities should be protecting individuals, protecting devices and protecting networks.

1.1 Protecting Individuals: Traditionally, personal security is protected by both the individual taking decisions to ensure that he or she is free from interference, and is also protected by institutions, including governments and companies, who may be gatekeepers to enable that security. It is often associated with physical security (of our physical selves and of our property/belongings) – are my home and possessions and finances safe and are transgressors held to account? Is my body safe from violation, and those of my loved ones?

With increased use of technologies to protect our security and safety, the integrity of those technologies has a direct relationship to our personal security. Our health data or financial data, when vulnerable, leave us feeling vulnerable but also open us to attacks by others. The disclosure of our data not only provides methods to place our physical selves at risk but also gives rise to new risks, e.g. fraud or blackmail.

Personal data is valuable. The value of the data is exactly why companies and governments want to collect, access, and mine it, and criminals want to steal it. Many "cyber crimes" have a common goal: To make money. Gaining access to an individual's bank or PayPal account, or any account that stores credit card details, is lucrative. Criminals can extort money from an individual or business by installing "ransomware" on a device, which allows an attacker to remotely take over a device, encrypt or delete files and demand a ransom from the owner to return access to its data. For example, the ransomware known as WannaCry spread globally by exploiting a vulnerability in Windows software, and impacted hospitals in the UK, banks in Russia and China, a telecommunications company in Spain, railways in Germany and other businesses.[3]

Some of these "cyber crimes" are carried out by "social engineering", that is getting a target to behave in a certain way that is contrary to his or her security interests, often through subversion. For example, the goal of a "phishing" email can be to convince someone, through the air of legitimacy, to reveal a password or more information about themselves that an attacker can use to gain access to his or her account. Or the goal could be to convince someone to click on a malicious link that allows malware to be installed on their device. Convincing a company employee or customer service agent

[2] F. Schneider, E. Sedenberg, D. Mulligan, Public Cybersecurity and Rationalising Information Sharing, Opinion Piece for the International Risk Governance Center (IRGC). Lausanne: IRGC (2016) https://www.cs.cornell.edu/fbs/publications/publicCybersecRisks.pdf

[3] Alex Hern and Samuel Gibbs, What is WannaCry Ransomware And Why Is It Attacking Global Computers?, The Guardian, 12 May 2017 https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20 Agamoni Ghosh and India Ashok, WannaCry: List Of Major Companies And Networks Hit By Ransomware Around The Globe, International Business Times, 16 May 2017 http://www.ibtimes.co.uk/wannacry-list-major-companies-networks-hit-by-deadly-ransomware-around-globe-1621587 Sam Jones and Tim Bradshaw, Global Alert to Prepare For Fresh Cyber Attacks, The Financial Times, 14 May 2017 https://www.ft.com/content/bb4dda38-389f-11e7-821a-6027b8a20f23

to reveal information about a person or a company might help the attacker gain access to their accounts or the company's networks. The point of social engineering is that it circumvents security systems without breaking them technically.

But this social engineering technique is not only used by common "cyber criminals". State-sponsored hacking uses the same tactics to acquire personal data, including in bulk, as well as to gain access to whole networks, carry out reconnaissance missions and ultimately attack critical infrastructure (see Section 1.4 below).

Experts have spoken of the need to treat cyber security in the same way as public health, and invest in "cyber health" or "cyber hygiene" programmes to teach people of the dangers of the actions outlined above.[4] Lack of basic "cyber hygiene" (e.g. using short and easily guessable passwords or the same passwords for many accounts, not using password protection or two-factor authentication, or failing to install the latest software updates) and lack of awareness of social engineering methods (e.g. a user clicking on a malicious link, opening an infected email attachment, inserting an infected USB or CD into a computer) are the most frequent ways that security is compromised and individuals, devices and networks fail to be protected.[5]

While educational and awareness-raising programmes on the above risks are important, governments tend to overly focus on the individual as the 'weakest link', as a threat to cyber security whose behaviour needs to be 'fixed'. Cyber security is about more than trying to convince people to change the online habits that leave them vulnerable to fraud, scams, or phishing.

Putting the onus on individuals to protect themselves plays down the responsibility of companies, governments and other stakeholders. For example, companies need to design their products and services with privacy and security embedded at the earliest stages. Governments need to create incentives for this to happen.

The very systems that protect people and their data also need protection. Across our societies we rely on security and safety systems to resist against attack or failure. Computing systems are part of the safety mechanisms in our cars, from anti-lock brakes, lane departure assistance, and now obstacle detection. In turn, our concerns about security must focus on the very integrity of the protection and control systems. Ensuring our systems, as deployed, are truly secure is essential to ensuring that data everywhere can be secured and in turn that people are safe. Security at this level is very hard, but there are a few necessary measures to contribute to safe systems. First, both industry and government must embrace and promote the use of strong end-to-end encryption rather than undermining it. Promoting best practice and reducing the level of risk that could arise to our systems should be a priority of the security agendas. Second, we must promote the testing of the claims about the effectiveness

[4] European Network and Information Security Agency (ENISA), Cyber Hygiene, 7 February 2017 https://www.enisa.europa.eu/publications/cyber-hygiene See also, Brookings Institute, Cyber Security Threats and Basic Cyber Hygiene, 3 January 2014 https://www.brookings.edu/on-the-record/cybersecurity-threats-and-basic-cyber-hygiene/

[5] UK National Cyber Security Centre, Common Cyber Attacks: Reducing the Impact, January 2016 https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/common_cyber_attacks_ncsc.pdf

of security in systems, but legal restrictions that prevent them from doing so need to be reconsidered. Just as cars' physical safety mechanisms are tested regularly in a MOT, to protect people, we must test software. This will be explored later in the paper.

1.2 Protecting Devices: Protecting individuals is closely tied with device security. Increasingly our devices are being connected to the internet, at an alarming rate, even as the amount of data they store increases and the security mechanisms protecting the devices are too often untested.

Updating the software on a device, such as a mobile phone or computer, with the latest security patches is an essential practice for individuals and businesses seeking to protect themselves against cyber attacks. Governments around the world must encourage people to download and install software security updates as a critical cyber security measure.[6] Again, this approach puts the burden on the individuals, suggesting that users are failing to install updates provided to them. However, a recent study on Android vulnerabilities found that it is device manufacturers that fail to provide updates to users in order to fix critical vulnerabilities, rather than users failing to install them.[7]

Further, while there is significant focus on the devices, such as smartphones and computers, over which individuals have elements of control over, there is a need to look more closely at other devices over which individuals have much more limited interaction and control. These include network routers that let people decide who and what has access to their home networks,[8] or a range of household and office appliances such as energy meters and printers. As is frequently reported, the list of products connected to the internet grows every day, creating a web of connected devices—commonly known as the "Internet of Things"—that transmit their data to the internet. A massive amount of data can be stored on those devices, or accessed via these devices.

Securing these devices should therefore be a key cyber security objective, both for the risk they pose in relation to the personal data they generate, collect and transmit and for the security risks they pose as integrated in or as part of a network (see Section 1.3 below). While it is cheap to connect devices to the internet, it is generally agreed among security experts that the security of these devices is very poor.[9] Many devices have poor security such as no or default passwords, and are difficult or even impossible for everyday users to change.[10] Therefore, many of these internet-connected devices are vulnerable, and in turn, a potential threat to personal and network security.

6 One UK Home Office cyber security education campaign explains: "Software updates contain vital security upgrades which help protect your device from viruses and hackers [..,] While it's easy to hit 'cancel' and go back to what you're doing, the few minutes it takes to download and install the software updates could save you an enormous amount of time and trouble in the long run. https://www.cyberstreetwise.com/software-updates"

7 Daniel R Thomas, Alastair R Beresford and Andrew Rice, Security Metrics For The Android Ecosystem, University of Cambridge, 12 October 2015 https://www.cl.cam.ac.uk/~drt24/papers/spsm-scoring.pdf

8 Matthew Braga, Oft-forgotten, Why The Humble Router Remains One Of The Most Insecure Devices In Your Home, CBC News, 9 March 2017 http://www.cbc.ca/beta/news/technology/routers-cia-wikileaks-cyber-security-insecure-1.4017033

9 Bruce Schneier, Click Here To Kill Everyone, 27 January 2017 http://nymag.com/selectall/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html

10 Lorenzo Franceschi-Bicchierai, The Internet of Things Sucks So Bad Even 'Amateurish' Malware Is Enough, Motherboard, 3 October 2016 https://motherboard.vice.com/en_us/article/internet-of-things-malware-mirai-ddos

Security expert Bruce Schneier has observed that big companies like Apple spend a lot of money on testing security features (and have indeed clashed with governments about it, for example in the Apple v FBI case[11]) as the company views having better security as a competitive advantage. However, Schneier says,

> **"Unfortunately, this isn't true of embedded systems like digital video recorders or home routers. Those systems are sold at a much lower margin, and are often built by offshore third parties. The companies involved simply don't have the expertise to make them secure."[12]**
>
> Security expert Bruce Schneier

In early 2017, the US Federal Trade Commission (FTC) filed a lawsuit against Taiwan-based computer networking equipment manufacturer D-Link and its U.S subsidiary over alleged failures to reasonably secure its wireless routers and web cams, leaving them vulnerable to hackers.[13]

Policy-makers and regulators need to address how they will encourage connected devices and product manufacturers to make devices more secure, particularly when there is currently no market incentive to do so. Regulators need to have better tools to monitor and ensure compliance with standards of security and privacy. Civil society needs to ready itself to present the case for change.

1.3 Protecting Networks: Software updates do not just apply to an individual's devices, but also those running on a network, such as a router. If a device is compromised, a whole network is also at risk.[14]

Good network security means reducing the attack surface and then allowing the right people through the right devices to access the right services on a network, and keeping everyone and everything else out. Protecting and defending a network can mean protecting a home Wi-Fi connection, a company's intranet, a telecommunications network accessed by the public, a bank's network, an industrial control system (ICS) in a

[11] See Privacy International intervention: In the Matter of the Search of an Apple iPhone Seized during the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 ("Apple v. FBI") https://www.privacyinternational.org/node/1002

[12] Bruce Schneier, Click Here To Kill Everyone, 27 January 2017 http://nymag.com/selectall/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html

[13] Federal Trade Commission (FTC), FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras, 5 January 2017. https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate
UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF CALIFORNIA SAN FRANCISCO DIVISION Case 3:17-cv-00039: https://www.ftc.gov/system/files/documents/cases/170105_d-link_complaint_and_exhibits.pdf

[14] Following a systems breach at the US Chamber of Commerce in 2011, the chamber worked with the FBI to secure its systems. Months later, "the chamber discovered that Internet-connected devices – a thermostat in one of its corporate apartments and a printer in its offices – were still communicating with computers in China." Nicole Perlroth, Hackers in China Attacked The Times for Last 4 Months, New York Times, 20 January 2013 http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html via Ben Buchanan, The Cybersecurity Dilemma, Hurst & Company London, 2016 p45

factory, or a nation's critical infrastructure such as a power grid. In the future, defending the security of the internet will mean having to get all of these right, simultaneously.[15]

The failure to adequately protect network security was famously demonstrated in October 2016 when malware, known as Mirai, powered a huge denial of service (DDoS) attack, enabled by a botnet of hundreds of thousands of infected internet connected devices. It targeted the Dyn network that hosted a range of popular websites such as Twitter, Netflix and the New York Times, which were made inaccessible for a time.[16] Being unable to access these websites is inconvenient, but the real significance lies in the fact that the malware targeted and denied access and service to sections of a global network. This type of attack therefore raises questions about the security of network infrastructure as a whole. Denial of service at this scale could cripple critical infrastructure, particularly as we continue to connect systems to networks.

Protecting and defending individuals, devices and networks should form the basis of any cyber security strategy. They are interlinked and interdependent, which the example below explores.

1.4 Example: The 2015 Attack on Ukraine's Electricity System

An example where failures to protect individuals, devices and network security led to a real world impact is the cyber attack targeting the Ukrainian electricity system in December 2015, which left 225,000 customers without electricity for several hours. An analysis noted that the attack was co-ordinated and sophisticated; the attackers were patient and planned the attack over many months. Many opportunities existed for the attackers to execute the attack, by finding vulnerabilities in personal, device and network security.[17]

The attacks began in the Spring of 2015 with a 'spear-phishing' campaign that targeted specific IT staff and system administrators at three separate electricity companies in Ukraine with emails that contained malicious Microsoft Office documents. When the targets opened the attachments, a pop up window encouraged the targets to click to "enable macros" on the document, a legitimate feature of Microsoft Word, but which allowed the malware to exploit macro functionality to enable installation. By installing malware, the attackers now had remote access to the targeted systems and could move through them undetected.[18]

15 For example, see the reaction from the Government of Pakistan and civil society that the NSA had harvested millions of phone, internet and call data through the Fairview and SKYNET programmes and GCHQ in the UK had hacked the Pakistan Internet Exchange. See Privacy International, Tipping The Scales: Security & Surveillance In Pakistan, July 2015 (p6-7) https://www.privacyinternational.org/sites/default/files/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdf.

16 Dyn, Dyn Analysis Summary of Friday October 21 Attack, 26 October 2016 http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/ New York Times, Hackers Used New Weapons to Disrupt Major Websites Across the UK, 21 Oct 2016 https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html?_r=0

17 Unless otherwise specified, the description draws on SANS ICS/E-ISAC report, Analysis of the Cyber Attack on the Ukrainian Power Grid, 18 March 2016 https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

18 "The method is notable because most intrusions these days exploit a coding mistake or vulnerability in a software program; but in this case the attackers exploited an intentional feature in the Microsoft Word program. Exploiting the macros feature is an old-school method from the 90's that attackers have recently revived in multiple attacks". Kim Zetter, Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, Wired, 3 March 2016 https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ For a description on how malware can be distributed through macros see, Lucian Constantin, Macro-based Malware is Making a Comeback, Researchers Warn, Computerworld, 7 January 2015 http://www.computerworld.com/article/2866055/macro-based-malware-is-making-a-comeback-researchers-warn.html

Over a period of months attackers used their access to these systems to map the networks and steal log-in credentials. Authorised employees were not required to use two-factor authentication to log-in remotely to the network that controlled the grid, so once the attackers had obtained the right credentials they were able to gain access to other parts of the systems.[19] Once the attackers had located the systems they wanted to switch off, they made themselves known. In a 2016 talk, security expert Mikko Hypponen described what happened next,

"One of the operators was at his workstation and he realised the computer mouse was not working… but then he noticed that although his mouse did not work, the cursor on the screen was moving anyway. And this is a bad sign. He tried getting control of his computer but realised there was someone else operating the computer and other operators were facing the same problem. And they watched as an unknown attacker used their systems to turn off backup power generators one by one, then start clicking relays which actually turn power off in different parts of the electricity grid in the Ukraine. They followed this for a couple of minutes until they saw the unknown ghost operator then click the buttons to turn off the back up power of the building they were in themselves. They clicked off the power and the operators were left in darkness."[20]

Security expert Mikko Hypponen

Not only that, the attackers overwrote the firmware on some power converters leaving them inoperable and unrecoverable. Then they used malware to wipe files from operator stations to such an extent that they could not reboot.[21] To finish off for good measure, the attackers used the electricity company's own telephone system to conduct a DDoS attack on the company's customer call centre, which prevented anyone from reporting the blackout.[22]

This example illustrates a range of techniques to exploit weaknesses in personal, device and network security. It demonstrates the importance of all three aspects working together, and the disastrous results when they don't. Policy makers should not merely focus on the individual as the "weakest link" but ensure they take a holistic approach to cyber security by emphasising the importance of simultaneously protecting individuals and their data, protecting devices, and protecting networks.

19 Kim Zetter, Wired, 3 March 2016

20 IVY TV, What World Renowned Computer Security Expert Mikko Hypponen Thinks You Need To Know About Fighting Hackers, December 2016. See quote at 31 mins 30 secs http://tv.ivy.com/how-to-fight-hackers/

21 Kim Zetter, Wired, 3 March 2016

22 SANS ICS/E-ISAC (p2)

PART 2: Global Cyber Security Policies, Practices and Laws That Undermine Cyber Security

In contrast to Part 1's description of cyber security as prioritising the protection of individuals, devices and networks, governments often do not prioritise addressing the root problem of insecure systems and acting to secure them. Governments continue to adopt policies and pass laws that undermine cyber security as a whole and therefore place human rights at risk. Below we share some findings from research by Privacy International and our international network of partners about policies, laws and practices in their countries. Privacy International believe the below issues are the starting point for engaging in cyber security discussions, and the building blocks for effective engagement.

2.1 Cyber Security Strategies That Fail to Prioritise Individual, Device and Network Security

Traditionally, an indication of cyber security priorities is outlined in a government's cyber security strategy, if the country has one. Priorities vary from country to country. For example, while Kenya's focuses on private sector growth,[23] Colombia's calls for an increase in law enforcement and intelligence agencies capabilities.[24] This approach fails to address what a government intends to do to ensure protection of individuals, devices and networks, as outlined in Part I.

Governments tend to frame cyber security under their own preferred terms and to match their political aims. Worryingly, some governments often bundle regulation of online expression under the banner of cyber security, e.g. using it as an opportunity to regulate what they perceive as hate speech.[25] If a government prioritises policing online behaviour, surveillance of content, or censorship as cyber security issues, it is likely to weaken rather than strengthen security, e.g. limit encryption and there is a good chance that essential work will be under-resourced or ignored, such as identifying vulnerabilities and securing critical infrastructure and supporting security research.

2.2 Enacting Repressive Cyber Crime Laws

In 2016, Privacy International published the State of Privacy reports, co-written by partners in 17 countries. In the State of Privacy reports, many partners identified cyber security as a government priority in their country, but also identified repressive cybercrime laws that often deny privacy online or violate freedom of expression.[26]

23 Kenya National Cyber Security Strategy https://www.thegfce.com/documents/publications/2017/01/26/kenya-national-cybersecurity-strategy

24 See State of Privacy report for Colombia https://www.privacyinternational.org/node/977#toc-7 https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf The Organisation of American States (OAS) has a dedicated Cyber Security programme, which is helping a number of countries to develop cyber security strategies, http://www.oas.org/en/member_states/

25 See section 17 on hate speech in the draft Cybercrime and Computer Related Crimes Bill in Kenya.

26 Privacy International State of Privacy reports https://www.privacyinternational.org/reports/state-of-privacy

For example, using encrypted messaging services is illegal in Pakistan,[27] and using them in Morocco will land you in prison and a $10,000 fine.[28] The Computer Misuse Act in Uganda has been used to criminally charge a journalist investigating government corruption.[29] The Computer Crimes Act in Thailand has been used to prosecute cases of "lese-majeste", involving expression about the Royal Family that is perceived as negative.[30] The Prevention of Electronic Crimes Act in Pakistan regulates what is perceived as 'hate speech'.[31] Although cyber security strategies and cyber crime laws are separate instruments, they often overlap in practice. While States may have good intentions in producing cyber security strategies to protect economic interests, critical infrastructure etc., the cybercrime laws that are enacted to deal with "gaps" in legislation often have little alignment with cyber security outcomes. Privacy International and partners will continue to explore this in future research and publications.

2.3 Lack of Security Surrounding Data Intensive Programmes

Privacy International and partners have observed that governments are keen to develop data-intensive projects, but lack consideration for securing the personal data those projects generate. For example, some countries without data protection laws are developing projects including smart cities (e.g. India and Indonesia) or biometric voter registration systems (e.g. Kenya).

Data breaches continue globally, and the numbers involved are staggering. Continued scrutiny of the Aadhaar project in India has revealed serious flaws in security, where Aadhaar numbers were published alongside personally identifiable information on several government websites.[32] The personal information of over 93 million voters in Mexico,[33] including home addresses, were openly published on the internet after being taken from a poorly secured government database. This can be highly sensitive information; in Mexico for instance there are gross abuses of rights, including up to 100,000 people are reportedly kidnapped each year.[34] Similarly, the personal information of over 55 million Filipino voters were made publicly available, the biggest data breach in the Philippines' history.[35] A database containing the records of 650,000 patients in Sao Paolo, Brazil was made public, putting people at a variety of risks, from becoming victims of identity theft to persecution e.g. when the identities of women undergoing abortions were exposed.[36]

27 State of Privacy report for Pakistan (Section on Encryption) https://www.privacyinternational.org/node/970

28 State of Privacy report for Morocco https://www.privacyinternational.org/node/971

29 Uganda v. Nyakahuma (2013) http://www.ulii.org/ug/judgment/high-court-criminal-division/2013/30-0 The case was dismissed in 2015 due to lack of evidence https://freedomhouse.org/report/freedom-press/2016/uganda

30 Privacy International, Compliant or Complicit? Thai Government made American industry complicit in speech prosecution, 17 November 2015 https://privacyinternational.org/node/674

31 See Section 10a on hate speech in the Prevention of Electronic Crimes Act in Pakistan.

32 The Centre for Internet and Society (CIS) Information Security Practices of Aadhaar (or lack thereof): documentation of public availability of Aadhaar Numbers with sensitive personal financial information http://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1

33 Dell Cameron, Private Records Of 93.4 Million Mexican Voters Exposed In Data Breach, The Daily Dot, 22 April 2016 http://www.dailydot.com/layer8/amazon-mexican-voting-records/

34 Vladimir Hernandez, Our World: Kidnapped in Mexico, 15 March 2017 http://www.huffingtonpost.com/vladimir-hernandez/our-world-kidnapped-in-mexico_b_9462258.html

35 State of Privacy report for The Philippines https://www.privacyinternational.org/node/969#toc-5

36 State of Privacy report for Brazil https://www.privacyinternational.org/node/979#toc-5

In sum, companies and governments build systems, devices, networks and services that generate and accumulate vast data stores without proper regard to risk, security, or data minimisation. With no legal obligations to protect personal data against unauthorised access, there will be consequences, as many people are left vulnerable to excessive data being collected on them and that data is poorly secured and ultimately stolen. Data breaches have a knock on effect for a country's cyber security as they cause people to lose trust in systems, cost the economy greatly and direct resources towards retrospectively securing systems that should have been built securely from the outset.

2.4 Lack of Security Information from the Private Sector

Companies providing products and services are generally not forthcoming with information about the technologies they sell and their systems specifications, particularly with regards to security. Devices are generating data that users are unaware of, let alone understand how to secure – raising challenges for data protection and consumer protection regimes. There is huge pressure on consumers to accept without question that companies and governments can access data in ways that we do not fully understand. Without these protections, we do not have a way to gauge the security considerations in the deployment of increasingly complex systems.

What should be established is an acceptable level of due diligence in investigating services of companies and their security history. In 2015, the US software company Oracle agreed to settle charges by the US Federal Trade Commission (FTC) that it deceived consumers about the security provided by updates to its Java platform, which is installed on over 850 million computers.[37] The UK ISP Talk Talk was fined a record £400,00 following their data breach.[38] But what about all the breaches we do not know of, and poor security postures that remain concealed by vague claims of 'taking security seriously.' There currently exists only industry's claims and a lack of clarity. That information gap is frequently filled by security researchers. However, those with the skills and expertise to test security features and search for vulnerabilities and test exploits are often prevented from legally doing so.

2.5 Restrictions on Security Research

As outlined earlier, security researchers generally agree that the security of connected devices is poor. However, those with the skills and expertise to test security features of products and services and discover vulnerabilities are often prevented from legally doing so, even under the protection of institutions like universities.[39] To test a company's assurances that, for example, a phone is secure, an independent researcher may be breaking the law or the terms of service of the technology.

37 Federal Trade Commission (FTC) Oracle Agrees to Settle FTC Charges It Deceived Consumers About Java Software Updates 21 December 2015 https://www.ftc.gov/news-events/press-releases/2015/12/oracle-agrees-settle-ftc-charges-it-deceived-consumers-about-java

38 Information Commissioner's Office (ICO) TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack, 5 October 2016 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/

39 Letter from Professor Ross Anderson, University of Cambridge, to UK Cards Association Re: Responsible Disclosure and Academic Freedom, 24 December 2010 http://www.cl.cam.ac.uk/~rja14/Papers/ukca.pdf

There are many examples of researchers being arrested or threatened with arrest for discovering and exposing vulnerabilities, particularly in the systems of big business.[40] A 2015 study by ENISA concluded that in the EU and US, the threat of prosecution under computer misuse legislations 'can have a chilling effect' with security researchers 'discentivise[d]' to find vulnerabilities.[41] Instead of prohibiting or discouraging the identification of security weaknesses, which is in the public interest, skilled individuals who can do this need to be incentivised and encouraged so that adversaries with the same skills do not deploy them to undermine individuals' security and privacy.

Until governments and regulators take an active approach to querying and exploring insecurity for the purpose of securing systems of everyone everywhere, then they are relying on unequal distribution of security knowledge and application which ultimately secures no-one.

2.6 Attempts to Weaken Encryption

Privacy International has written extensively about the importance of encryption for privacy and freedom of expression, underpinning the secure functionality of the internet and facilitating global online commerce.[42] Once the domain of the technologically savvy, end-to-end encryption is now readily available and a feature of some accessible communication applications such as Facebook's WhatsApp, OpenWhisperSystem's Signal, and Apple's iMessage. What's essential about end-to-end encryption is that the messaging content is secure even from the infrastructure provider itself – if these providers are compromised, the messages themselves should remain secure.

As encryption is increasingly used, some governments are seeking to limit its availability under the justification that they need to access encrypted communications in order to fight terrorism or prevent serious crimes, including the sexual abuse of children. Privacy International has repeatedly warned of the security risks of putting in 'backdoors' to encryption, that is, creating a weakness that allows governments (and other actors) to access encrypted information.

Building security is hard enough as it is – as this paper has explored above – but building insecurity into the systems for exceptional access by only some actors is even

40 Robert Lemos, Russian crypto expert arrested at Def Con, CNET, 2 March 2002 https://www.cnet.com/uk/news/russian-crypto-expert-arrested-at-def-con/
Ian Sample, Bankers fail to censor thesis exposing loophole in bank car security, The Guardian, 30 December 2010 https://www.theguardian.com/science/2010/dec/30/bankers-thesis-bank-card-security
Lisa O'Carroll, Car hacking scientists agree to delay paper that could unlock Porsches, The Guardian, 30 July 2013 https://www.theguardian.com/technology/2013/jul/30/car-hacking-ignition-injunction
Legal Threats Against Security Researchers website: http://attrition.org/errata/legal_threats/

41 ENISA, Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations (2015) https://www.enisa.europa.eu/publications/vulnerability-disclosure, p65-66. Via Audrey Guinchard, Transforming the Computer Misuse Act 1990 to support vulnerability research. Proposal for a defense to hacking as a strategy in the fight against cybercrime, 27 March 2017 https://ssrn.com/abstract=2946763

42 Privacy International, Securing Safe Spaces Online: Encryption, online anonymity and human rights (2015) https://www.privacyinternational.org/node/599
Written evidence submitted by Privacy International (IPB0040) to the UK Science and Technology Committee re: The Investigatory Powers Bill. Section 23, 24, 25: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25170.html

harder.[43] The problem is that once a vulnerability is created in a tool like end-to-end encryption to allow for this exceptional access, it can introduce new weaknesses that can be discovered and exploited by others across many different services.

High profile attacks on encryption from governments play on the worn-out security vs privacy dichotomy. Encryption is about security and safety. Cryptography is essential for safety. It is used to protect confidentiality, but it is used just as much for integrity and authentication—so that we can be sure of the legitimacy of the person or institution communicating with us and the integrity of the communication itself. Banks need encryption to protect transactions, businesses to protect against fraud, civil servants to work on national security matters, and human rights defenders and journalists to communicate with their sources. Cryptography is not only for humans to communicate with each other: it's also used for machine to machine communications. When you update the software on an app or a device you use, cryptography is what guarantees what you are downloading is definitely an update from the vendor and not a piece of malware.[44] The moment that key is shared with a government agency the whole process is compromised.[45]

When governments attack encryption it gives the impression to the public that law enforcement is helpless to fight terrorism or serious crime. But when a criminal uses encryption, law enforcement does not just give up their investigation. There are several documented "encryption workarounds"[46] available which do not rely on intercepting content while it is in transit. However, these methods do raise novel legal questions, particularly around the use of governments' own use of hacking to circumvent encryption.[47] As policy-making around encryption remains in its infancy, clashes between governments, companies and civil society will continue. But end-to-end encryption is here to stay, and will only become more accessible and widespread as our security needs increase particularly as the threats grow. All actors must work together to end this stalemate.

2.7 Government Hacking and The Identification of Vulnerabilities

Part 1 of the paper discussed different ways an individual's device or information can be hacked. Hacking of individual's devices is most often carried out by remotely

43 Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, Daniel J. Weitzner, Keys Under Doormats: Mandating Insecurity By Requiring Government Access To All Data And Communications 7 July 2015 https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf

44 Microsoft Safety and Security Centre, Watch Out For Fake Virus Alerts https://www.microsoft.com/en-us/safety/pc-security/antivirus-rogue.aspx

45 See Privacy International, Winning The Debate On Encryption- A 101 Guide For Politicians, 21 April 2017 https://medium.com/@privacyint/winning-the-debate-on-encryption-a-101-guide-for-politicians-4ff4353d427

46 Orin Kerr and Bruce Schneier, Encryption Workarounds, 20 March 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938033

47 Privacy International press release: Privacy International Files Amicus Curiae Brief In Case Challenging Warrant Authorising FBI To Hack Over 8,700 Devices, Mostly Located Outside The US, 10 February 2017 https://medium.com/privacy-international/press-release-privacy-international-files-amicus-curiae-brief-in-case-challenging-warrant-3b20880ab4c4

48 For further background on hacking, please see Privacy International's submission on the Equipment Interference Code of Practice (20 March 2015) Available from: https://www.privacyinternational.org/sites/default/files/PI%20and%20ORG%20Submission%20-%20Draft%20Equipment%20Interference%20Code%2020%20Mar%202015_0.pdf

accessing the target's device. This can be done in a variety of ways. A common method is through sending out malicious emails that gains access to passwords or get the user to undo security mechanisms and install malware, such as when the email recipient clicks on a link or opens a file contained in the email. Another vector is to identify vulnerabilities that exist in computer systems to develop an exploit, for instance to install malware, sometimes even without the affirmative participation of the user.[48]

The result of hacking is usually discussed in the context of data losses or data breaches, e.g. when voter databases are exposed, or criminals motivated by financial gain steal personal data. But hacking is increasingly becoming a surveillance tool for intelligence agencies and law enforcement. While it used to be considered a tool at the disposal of the most sophisticated and well-resourced intelligence agencies, increasingly hacking capabilities are accessible to nearly any government across the world, through the procurement of offensive hacking systems, such as those from companies like Hacking Team, Finfisher and NSO Group.

Much has been written in light of troves of documents released by groups such as ShadowBrokers regarding the hacking capabilities of intelligence agencies, particularly about software vulnerabilities known as "zero days"[49] and whether intelligence agencies are "stockpiling" them. The concern is that intelligence or law enforcement agencies, however, often have different priorities when they discover a vulnerability, and instead of disclosing them to the developer to fix, they could keep it secret it in order to use it offensively as part of a hacking attack, or they could stockpile it for future use. There are now additional questions about vulnerabilities and exploits being lost or stolen; the recent WannaCry ransomware included an exploit for a vulnerability in Microsoft software that was claimed to be stolen from the National Security Agency (NSA) and published as part of a cache released by ShadowBrokers.[50]

While an issue, the use of zero days needs to be put into the wider security context. Government hacking powers skews already confused government policy on cyber security. Are governments to focus on securing individuals, devices and infrastructure or are they to focus on how to undermine them?

First, because of its inherent, excessive interference with privacy posed by hacking, Privacy International questions whether the use of this technique for surveillance purposes can ever be consistent with human rights standards.

To protect cyber security, we wonder if there is ever a constrained use of the power to identify and stockpile vulnerabilities, or a constrained use of the power of a government to use phishing or other fraudulent methods that undermine cyber security?

[49] Zero day vulnerabilities are those unknown to the developer and get their name from the fact that, once identified, the developer has 'zero days' to fix them before attackers exploit the vulnerability.

[50] Martin Lee, Warren Mercer, Paul Rascagneres, and Craig Williams, Player 3 Has Entered the Game: Say Hello to 'WannaCry', 12 May 2017 http://blog.talosintelligence.com/2017/05/wannacry.html

[51] Spencer Ackerman, Snowden: NSA accidentally caused Syria's Internet blackout in 2012, The Guardian 13 August, 2014 https://www.theguardian.com/world/2014/aug/13/snowden-nsa-syria-internet-outage-civil-war See also The Cybersecurity Dilemma p76

Even beyond the zero-day debate, the use of hacking tools and even the tools themselves need to be rendered transparent. As instances, some of the government hacking examples in the public domain appear to have included accidental damage - for example a massive internet outage in Syria in 2012 appears to be not the result of an intentional attack, but of an NSA collection operation that targeted Syrian routers and went wrong.[51] The malware the US government used to infect Iranian nuclear facilities, Stuxnet, was later found on computers at the corporation Chevron.[52] Government agencies want to keep their hacking techniques secret so much that the FBI dropped a case against an alleged child pornography offender rather than disclose to the defense details of a hacking tool.[53]

While the chances are small that an individual will be targeted by a zero day that has been discovered or purchased by a nation state's intelligence agency, it is more likely that people will fall victim to a known vulnerability. This is a vulnerability which has been discovered but may not have been patched by the company. Even where a patch has been developed, the operating system or software may not have been updated so the user is still at risk. Some software is no longer widely supported by the developer, such as Microsoft Windows XP, which was targeted by the WannaCry malware. The attack was so severe Microsoft released an urgent patch for Windows XP and other platforms for all customers, even if they did not pay for continued support.[54]

Failure to address a known vulnerability disproportionately impacts people in global south countries who are more likely to be Android operating systems and using older devices which are no longer being provided with security updates, or the user is unable to pay to receive additional support. A recent study found that on average 87.7% of Android devices are exposed to at least one of 11 known critical vulnerabilities.[55] In terms of updates that would patch the vulnerabilities, the study found, "the main update bottleneck lies with the manufacturer, rather than Google, the operator or users." Manufacturers of devices are failing to provide updates, rather than operators failing to supply them or users failing to install them. As outlined earlier, a lack of security information from the private sector has created a very unequal playing field, or as the study puts it, "there is information asymmetry between the manufacturer, who knows whether the device is currently secure and will receive updates, and the consumer, who does not. Consequently there is little incentive for manufacturers to provide updates."[56]

There are likely thousands upon thousands of vulnerabilities that are known. When researchers and others discover vulnerabilities, they often report the vulnerability to the company responsible for the security of the equipment affected. Then the company must act to patch vulnerabilities and secure systems. While Privacy International believes that vulnerabilities should be identified so that they can be patched, there

52 Rachel King, Stuxnet Infected Chevron's IT Network, Wall Street Journal, 8 November 2012 http://blogs.wsj.com/cio/2012/11/08/stuxnetPinfectedPchevronsPitPnetwork/

53 Lily Hay Newman, The Feds Would Rather Drop A Child Porn Case Than Give Up A Tor Exploit, Wired, 7 March 2017, https://www.wired.com/2017/03/feds-rather-drop-child-porn-case-give-exploit/

54 Microsoft, Customer Guidance for WannaCrypt Attacks, 12 May 2017 https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

55 Daniel R Thomas, Alastair R Beresford and Andrew Rice, Security Metrics For The Android Ecosystem, University of Cambridge, 12 October 2015 https://www.cl.cam.ac.uk/~drt24/papers/spsm-scoring.pdf

56 Ibid, p8

must be substantial efforts to ensure that software updates are provided to and installed by users.

2.8 Framing Cyber Security as National Security

Some governments have chosen to frame cyber security as a national security issue. This approach generally signals a government's intention to make cyber security the domain of intelligence agencies. Experts have called this approach "securitisation."[57]

Privacy International is concerned about the consequences of framing cyber security predominately as a national security issue and its impact on public understanding of cyber security, opportunities for public debate, transparency, accountability, oversight and human rights. Much needed public debates are shrouded in secrecy if cyber security is to be framed as a national security issue, for example regarding the use of offensive and defensive hacking.[58] The Organisation of American States (OAS) have acknowledged this too, stating:

"In the LAC [Latin America and Caribbean] region, the army and the national security agencies have not been widely established as coordinators of cybersecurity policy development. This provides a positive window of opportunity to develop cybersecurity policies in multi-stakeholder platforms, including different governmental branches, academia, the technical community, civil society, and the private sector. LAC countries will be able to advance a new notion of cybersecurity that is not derived only from the military and defense domains, but also from human rights."[59]

Without the ability for civil society to verify the claims of government and industry, whether through legal means (e.g. knowing which vulnerabilities are explored and used and reported, knowing when hacking is deployed and under what circumstances to what consequence) or technical means (e.g. exploring the boundaries of networks, services or devices through security research), we are left with no understanding and no security.

2.9 Exclusion of Different Voices

Privacy International is of course not the only organisation that believes human rights are at the heart of cyber security. Yet civil society organisations, academics and independent technical experts are largely frozen out of the conversation when it comes to deciding on cyber security priorities, policies and laws. In many countries, there is currently little transparency on how decisions regarding cybersecurity strategies and cybercrime laws are made and by whom. Civil society and technologists rarely have a seat at the decision-making table.

---

57 Ron Deibert, Distributed Security as a Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace. Calgary: Canadian Defence and Foreign Affairs Institute, 2012 https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf

58 See Eireann Leverett, In Defense of Offensive Hacking Tools, Privacy International, 5 May 2017 https://medium.com/privacy-international/in-defense-of-offensive-hacking-tools-33c9922bde02

59 Organisation of American States (OAS) and Inter-American Development Bank, Cybersecurity Are We Ready in Latin America and the Caribbean? 2016 P7 https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean.pdf

This exclusion inevitably leads to an adversarial relationship between governments and civil society, resulting in many initiatives being sent back to the drawing board. In 2015, a draft encryption policy in India was withdrawn after 24 hours due to public outcry over the requirement for end users to store plaintexts of communications for 90 days.[60] In South Africa, civil society successfully prevented a draft cybercrime law from being passed due to the lack of a public interest defense and perceived criminalisation of journalists and whistleblowers.[61] In Pakistan, civil society organisations campaigned for 18 months to try and force a rethink of the Prevention of Electronic Crimes Bill.[62]

Cyber policy and law making is in its infancy and requires the input of different stakeholders. Truly effective security must be done as a collaboration and no one actor can claim to have the solution. This requires trust and efforts to understand different stakeholder perspectives.

60 Yuthika Bhargava, Government To Withdraw Draft Encryption Policy, The Hindu, 28 March 2016 http://www.thehindu.com/news/national/govt-to-withdraw-draft-encryption-policy/article7677348.ece

61 Privacy International State of Privacy report, South Africa https://www.privacyinternational.org/node/968#toc-7

62 Privacy International, How Not To Draft Legislation: Prevention of Electronic Crimes Bill From Bill to Act https://www.privacyinternational.org/node/1028

Conclusion

Good cybersecurity policies and practices put people and their rights at the centre, rather than undermining them. Cyber security should be considered a public good, in the same way as public health, for example, which promotes collective responsibility for the benefit of everyone. In a cyber security context, securing the individual helps secures everyone. When we argue for security, we argue for security for data, individuals, devices and networks.

When Governments argue for security they often argue for something different, often focusing on criminalising behavior through repressive cyber crime laws rather than the root problem of insecure systems. Governments largely prioritise surveillance systems over secure networks and criminalise those with the very skills that can help make us safer. Governments turn on technology and try to break the very tools that enable security and privacy to flourish, such as encryption. Companies and governments build systems, devices, networks and services that accumulate vast data stores without proper regard to risk, security, or data minimisation. This ultimately makes people less secure.

Building an effective framework where offensive and defensive strategies and tools work hand in hand will help establish some balance in cyber security policy. It is essential that we do so as the complexity of our systems increases and we build on top of existing systems we assume to be secure but are not. It's better to check the foundations of the house and ensure they are sound before the house collapses, and it takes a whole range of stakeholders and expertise to ensure this.

In prioritising the individual and protecting people, devices and networks, governments take advantage of a real opportunity - to give something technically complex a human element. In short, giving the tin man a heart. Until this landscape improves, cyber security will suffer.