GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

Cyber security, civil society and vulnerability in an age of communications surveillance

Alex Comninos and Gareth Seneque
Justus-Liebig University Giessen and Geist Consulting [1]
Comninos.org

Introduction

Cyber security is increasingly important to internet users, including stakeholders in governments, the private sector and civil society. As internet users increase, so does the amount of malware,[2] fuelled by ubiquitous smartphones and social networking applications offering new vectors for infection. Botnets – networks of infected devices controlled by malicious operators – are used as proxies to commit criminal acts including fraud and identity or data theft. According to the antivirus company Symantec, in 2013 data breach incidents resulted in the exposure of 552 million personal identities.[3] In May 2014, eBay announced that hackers had gained access to the personal data of 145 million customers and urged all customers to change their passwords.[4] Infrastructures connected to the internet, such as power grids, are also vulnerable, and severely lacking security updates. A growing "internet of things", which includes ubiquitous devices from sensors in homes and cars to medical technology, presents a plethora of new vulnerabilities to cyber security incidents.

Increasingly, states are establishing military "cyber units" or "cyber commands", many of which have offensive hacking capabilities.[5] Michael Hayden, a former director of both the CIA and the National Security Agency (NSA) has stated that Stuxnet, a state-sponsored computer worm discovered in 2011 and designed to attack and incapacitate nuclear reactors in the Natanz facility in Iran, marked "the crossing of the Rubicon" (a point of no return) for the use of state-sponsored malware.[6] A number of similar worms, some of which have implemented Stuxnet's source code, have arisen.[7]

Civil society organisations and human rights defenders are becoming victims of surveillance software. Some of this software is sold to law enforcement and intelligence agencies in repressive regimes. "Remote Access Trojans" can be bought both legally and on the black market, as well as downloaded for free, and are used to control mobile devices, laptops and computers remotely, capturing all the information input/viewed by the user. Such software has been used to target activists in Bahrain and Syria.[8]

Edward Snowden's disclosures of documentary evidence regarding mass surveillance by the NSA, Government Communications Headquarters (GCHQ) in the United Kingdom, and other intelligence agencies of the "Five Eyes"[9] countries have shown just how vulnerable the average netizen's communications are to interception and surveillance. The disclosures have also demonstrated how surveillance activities can negatively affect the cyber security of all internet users.

It is tempting to think that more "cyber security" would be a means of countering the global privacy invasion caused by mass surveillance. However, cyber security discourse is dominated by states and corporations and focuses mainly on their security, rather than the security of civil society and of internet users. Civil society needs a vision of cyber security that puts the digital security of internet users at the centre of its focus. Attaining cyber security that protects human rights, including the

[1] Alex Comninos is a doctoral candidate in the Department of Geography at Justus-Liebig University Giessen; Gareth Seneque is a Unix architect at Geist Consulting.

[2] Malware is malicious software that includes viruses, Trojan horses and spyware.

[3] Symantec 2014 Internet Security Threat Report, Volume 19. www.symantec.com/security_response/publications/threatreport.jsp

[4] Perlroth, N. (2014, May 21). eBay Urges New Passwords After Breach. *New York Times*. www.nytimes.com/2014/05/22/technology/ebay-reports-attack-on-its-computer-network.html

[5] Comninos, A. (2013). *A cyber security agenda for civil society: What is at stake?* Johannesburg: APC. www.apc.org/en/node/17320

[6] Healy, J. (2013, April 16). Stuxnet and the Dawn of Algorithmic Warfare. *The Huffington Post*. www.huffingtonpost.com/jason-healey/stuxnet-cyberwarfare_b_3091274.html

[7] Bencsáth, B. (2012). Duqu, Flame, Gauss: Followers of Stuxnet. Presentation at the RSA Conference Europe 2012, Amsterdam, the Netherlands, 10 October. www.rsaconference.com/writable/presentations/file_upload/br-208_bencsath.pdf

[8] McMillan, R. (2011, August 7). How the Boy Next Door Accidentally Built a Syrian Spy Tool. *Wired*. www.wired.com/wiredenterprise/2012/07/dark-comet-syrian-spy-tool

[9] The "Five Eyes" countries are Australia, Canada, New Zealand, the United Kingdom and the United States, which are part of a multilateral agreement on cooperation in signals intelligence.

right to privacy, while also ensuring an open and secure internet, will not be possible unless dominant discourses on cyber security radically change.

The problems with "cyber security"

The term "cyber security" often lacks clear definition. It is used as an umbrella concept covering a range of threats and responses[10] involving national infrastructure, internet infrastructure, applications and software, and users. Sometimes it is even used to refer to the stability of the state and political structures. The inexact terminology of cyber security "mixes legitimate and illegitimate concerns and conflates different types and levels of risk." This "prevents genuine objective scrutiny, and inevitably leads to responses which are wide-ranging and can easily be misused or abused."[11]Cyber security not only leads to overly broad powers being given to the state, it also "risks generating a consensus that is illusory" and not useful for the problems at hand.[12] We need to carefully unpack the relevant issues and develop "a clear vocabulary of cyber security threats and responses," so as to enable "targeted, effective, and rights-respecting policies."[13] If we do not, cyber security can be used by governments as a justification to censor, control or surveil internet use.

Viewing cyber security as an issue of national security is perilous and unhelpful. We should distinguish between, and not conflate, on the one hand, protecting computers, networks and information, and on the other hand using technological tools to achieve security objectives. Using "cyberspace as a tool for national security, both in the dimension of war fighting and the dimension of mass surveillance, has detrimental effects on the level of cyber security globally."[14] When cyber security is framed as a national security issue, issues regarding technology and the internet are *securitised* – brought onto the security agendas of states. This may be counterproductive. The state, law enforcement, military and intelligence agencies may not have the best skills or knowledge for the job. State actors may have a conflict of interest in securing information: militaries, for example, may want to develop offensive weapons, while intelligence agencies may rely on breaking or circumventing information insecurity in order to surveil better. Cyber security may also be used to protect state secrets, and criminalise whistleblowers as cyber security threats. Focusing on the state and "its" security, "crowds out consideration for the security of the individual citizen, with detrimental effects on the security of the whole system."[15]

Cyber security often disproportionately focuses on the protection of information, databases, devices, assets and infrastructures connected to the internet, rather than on the protection of connected users. Technological infrastructures and the assets of corporations are put at the centre of analysis, rather than human beings. Human beings are seen as a threat in the form of bad "hackers" or as a weak link in information systems, making mistakes and responding to phishing or "social engineering" attacks.[16] Putting humans at the centre of cyber security is important. A definition of cyber security as purely protecting information avoids ethical challenges. Cyber security should not protect some people's information at the expense of others. It should also not protect information about state secrets in order to enable mass surveillance and privacy invasion of individual users.

Cyber security and vulnerability

Cyber security discourse should focus more on information security *vulnerabilities*, rather than on threats and responses. This focus would help to delineate what constitutes a cyber security issue, avoid cyber security escalating to a counter-productive national security issue, and place a practical focus on the protection of all internet users.

A security vulnerability, also called a "bug", is a piece of software code that contains an error or weakness that could allow a hacker to compromise the integrity, availability or confidentiality of information contained, managed or accessed by that software.[17] When a vulnerability is discovered, a malicious hacker may make an "exploit"[18] in order

[10] Center for Democracy and Technology. (2013). *Unpacking "Cybersecurity": Threats, Responses, and Human Rights Considerations*. https://cdt.org/insight/unpacking-cybersecurity-threats-responses-and-human-rights-considerations

[11] Kovacs, A., & Hawtin, D. (2014). Cyber Security, Surveillance and Online Human Rights. Discussion paper written for the Stockholm Internet Forum, 27-28 May. www.gp-digital.org/publication/second-pub

[12] OECD. (2012). *Non-governmental Perspectives on a New Generation of National Cyber security Strategies*, p 6. dx.doi.org/10.1787/5k8zq92sx138-en

[13] Center for Democracy and Technology. (2013). Op. cit.

[14] Dunn Cavelty, M. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*, April.

[15] Ibid.

[16] Dunn Cavelty, M. (2014). Op cit. Wikipedia defines social engineering as "psychological manipulation of people into performing actions or divulging confidential information." https://en.wikipedia.org/wiki/Social_engineering_(security) A common example is phishing.

[17] For a definition upon which this is based, see Microsoft, Definition of a Security Vulnerability: technet.microsoft.com/en-us/library/cc751383.aspx

[18] An exploit is a "is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior," and does not require advanced technical skills to use. https://en.wikipedia.org/wiki/Exploit_(computer_security)

to compromise data or access to a computer. Malware – viruses and Trojan horses – require exploits (or collections of exploits) that take advantage of vulnerabilities. Expertise in fixing vulnerabilities is improving but not keeping up with the pace of the growth. Compared to 15 years ago, all popular and contemporary desktop operating systems (Windows, Linux and Mac) offer regular automated security updates which fix or "patch" known vulnerabilities. While we are finding more vulnerabilities in code and viruses than ever before, we are also getting better at finding them. At the same time we keep producing more software code, meaning that the net number of vulnerabilities is increasing.[19]

Viruses and botnets, including Stuxnet and other state-sponsored malware, require vulnerabilities to work. Finding and fixing vulnerabilities contributes to a safer and secure internet, counters surveillance and can even save lives. For example, a vulnerability in Adobe's Flash software was recently used against dissidents in Syria.[20]

There are two categories of vulnerabilities, each requiring different user and policy responses: zero-days and forever-days. Zero-days are vulnerabilities for which there is no available fix yet, and may be unknown to developers. Forever-days are vulnerabilities which are known of, and either do not have a fix, or do have a fix in the form of a patch or an update, but they are for the most part not applied by users.

Zero-day vulnerabilities

When a zero-day is found, the original software developer should be notified so that they may find a fix for the vulnerability and package it as a patch or update sent out to users. Furthermore, at some stage, users of the affected software that are rendered vulnerable should also be informed, so they can understand if they are or have been vulnerable and take measures to recover and mitigate for the vulnerability.

Throughout the history of computers, "hackers"[21] have sought to use technology in ways that were not originally intended. This has been a large source of technological innovation. Hackers have applied this logic to computer systems and have bypassed security and found vulnerabilities for fun, fame, money, or in the interests of a more secure internet. It is because of people that break security by finding vulnerabilities that we can become more secure. A problem for cyber security is that "good" (or "white hat") hackers or "security researchers" may not be incentivised to find zero-days and use this knowledge for good. Rather than inform the software vendor, the project involved, or the general public of a vulnerability, hackers may decide not to disclose it and instead to sell information about a vulnerability, or package it as an *exploit* and sell it.

These exploits have a dual use: "They can be used as part of research efforts to help strengthen computers against intrusion. But they can also be weaponised and deployed aggressively for everything from government spying and corporate espionage to flat-out fraud."[22] There is a growing market for zero-days that operates in a grey and unregulated manner. Companies sell exploits to governments and law enforcement agencies around the world; however, there are concerns that these companies are also supplying the same software to repressive regimes and to intelligence agencies. There is also a growing black market where these exploits are sold for criminal purposes.[23]

Forever-day vulnerabilities

Forever-days (or "i-days"/"infinite-days") are also a serious cyber security problem. Forever-day vulnerabilities either take a long time to get fixed, or never get fixed, or are fixed but users do not update or patch the relevant software. While they can affect internet users, they can also affect industrial control systems (ICSs), which control infrastructures such as power grids and power plants, as well as machinery in factories, for example, in pharmaceutical plants. ICSs require large investments in equipment that is supposed to last for many years. Operators of ICSs usually cannot afford to update their systems regularly. In addition to zero-days, well-documented forever-day vulnerabilities in Siemens controllers allowed the Stuxnet virus to infect the Natanz nuclear reactors in Iran.[24] Forever-days

[19] McGraw, G. (2012). Cyber War, Cyber Peace, Stones, and GlassHouses. Presentation at the Institute for Security, Technology, and Society (ISTS), Dartmouth College, Hanover NH, USA, 26 April. www.ists.dartmouth.edu/events/abstract-mcgraw.html , www.youtube.com/watch?v=LCULzMa7iqs

[20] Fisher, D. (2014, April 28). Flash zero day used to target victims in Syria. *Threat Post*. threatpost.com/flash-zero-day-used-to-target-victims-in-syria

[21] "Hacker" is used here in its original usage to refer to people who playfully use technological systems, rather than in its current pejorative and widely used usage.

[22] Gallagher, R. (2013, January 16). Cyberwar's gray market. *Slate*. www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html; Grossman, L. (2014, July 21). World War Zero: How Hackers Fight to Steal Your Secrets. *Time*. time.com/2972317/world-war-zero-how-hackers-fight-to-steal-your-secrets

[23] Gallagher, R. (2013, January 16). Op. cit.

[24] Zetter, K. (2011, August 4). Serious security holes found in Siemens control systems targeted by Stuxnet. *Ars Technica*. arstechnica.com/security/2011/08/serious-security-holes-found-in-siemens-control-systems-targeted-by-stuxnet Stuxnet also made use of four zero-days; see Kushner, D. (2013, February 26). The Real Story of Stuxnet. *IEEE Spectrum*. spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

in ICSs raise the spectre of "cyber war", in which, for example, "terrorists" could attack and cripple power lines. The solution however requires software updates, rather than military involvement.

Windows XP is perhaps one of the most important cyber security threats this year for government, civil society and critical national infrastructures connected to the internet. Many industrial control systems are running on Windows XP. The security updates for Windows XP expired this year, meaning that computers running XP will be exposed to thousands of vulnerabilities.[25] It is hard for governments and civil society to say goodbye to Windows XP, especially in the developing world, and in low-budget environments. The software is easy to use, runs on old computers, can be customised, runs modern web browsers, and allows its users to fully participate in the information society using a 13-year old operating system. In April 2014, XP use still accounted for over 18% of desktop PC use.[26] The UK and Dutch governments and some corporations have recognised the severity of the problem, and are actually paying Microsoft for private updates.[27]

The Heartbleed vulnerability

April 2014 marked an important watershed for awareness of vulnerabilities, with what has been described as one of the most catastrophic security vulnerabilities ever discovered: Heartbleed.

Heartbleed was a vulnerability in an open source software project called OpenSSL, which is used to establish encrypted connections between websites and browsers. According to *Forbes* magazine, "Some might argue that it is the worst vulnerability found (at least in terms of its potential impact) since commercial traffic began to flow on the Internet."[28] The vulnerability allowed a potential hacker to steal private encryption keys from a web server, and by doing so, to hijack login credentials or decrypt sensitive information, leaving two-thirds of the web open to eavesdropping.[29] The vulnerability existed for over two years, making a large proportion of the internet vulnerable. Heartbleed has not just had negative effects. It is the first vulnerability with its own logo,[30] and coverage of it extended far beyond technical audiences, engendering understanding of vulnerabilities among people who would usually not be aware of them. It has also resulted in more human and financial investment into OpenSSL development and alternatives.[31]

Open source software promises, in theory, to make software less vulnerable, as the code is open for anyone to review and to look for vulnerabilities. Open source software, however, will not provide security unless there are enough eyes on the code. Heartbleed was an open source project, and anyone could review the code, but it was underfunded and understaffed, and there were not enough reviewers of the code from outside the project. Symptomatic of this, the update that would introduce Heartbleed was finalised an hour before midnight on New Year's Eve 2011, and would go unnoticed for two years.

The relevance of Snowden's disclosures to cyber security

The scope and reach of the NSA's surveillance is important. The NSA's surveillance posture is – as has been repeated by General Keith Alexander, and is reflected in the NSA slide in Figure 1 – to "collect it all":[32] from undersea cable taps, to Yahoo video chats, to in-flight Wi-Fi, to virtual worlds and online multiplayer games like Second Life and World of Warcraft. The NSA has at least three different programmes to get Yahoo and Google user data. This shows that they try to get the same data from multiple mechanisms.[33] With the GCHQ under the MUSCULAR programme it hacked into the internal data links of Google and Yahoo[34] for information

[25] Windows XP Embedded (XPe), which should be the preferred operating system for ICSs, should receive updates till 2016. There is a suggested but unofficial workaround to make XP receive XPe updates, which may be useful for those with no other option (see: arstechnica.com/information-technology/2014/05/update-enabling-windows-xp-registry-hack-is-great-news-for-xp-die-hards).

[26] Newman, J. (2014, May 1). Windows XP refuses to go down without a fight. *PC World*. www.pcworld.com/article/2150446/windows-xp-usage-wont-go-down-without-a-fight.html

[27] Gallagher, S. (2014, April 6). Not dead yet: Dutch, British governments pay to keep Windows XP alive. *Ars Technica*. arstechnica.com/information-technology/2014/04/not-dead-yet-dutch-british-governments-pay-to-keep-windows-xp-alive

[28] Steinberg, J. (2014, April 10). Massive Internet Security Vulnerability – Here's What You Need To Do. *Forbes*. www.forbes.com/sites/josephsteinberg/2014/04/10/massive-internet-security-vulnerability-you-are-at-risk-what-you-need-to-do

[29] Goodin, D. (2014, April 8). Critical crypto bug in OpenSSL opens two-thirds of the Web to eavesdropping. *ARS Technica*. arstechnica.com/security/2014/04/critical-crypto-bug-in-openssl-opens-two-thirds-of-the-web-to-eavesdropping

[30] heartbleed.com/heartbleed.svg

[31] There are two new "forks" or versions of OpenSSL that promise to be more secure. One is called BoringSSL and is developed by Google, and one is called LibreSSL and is developed by the OpenBSD Project.

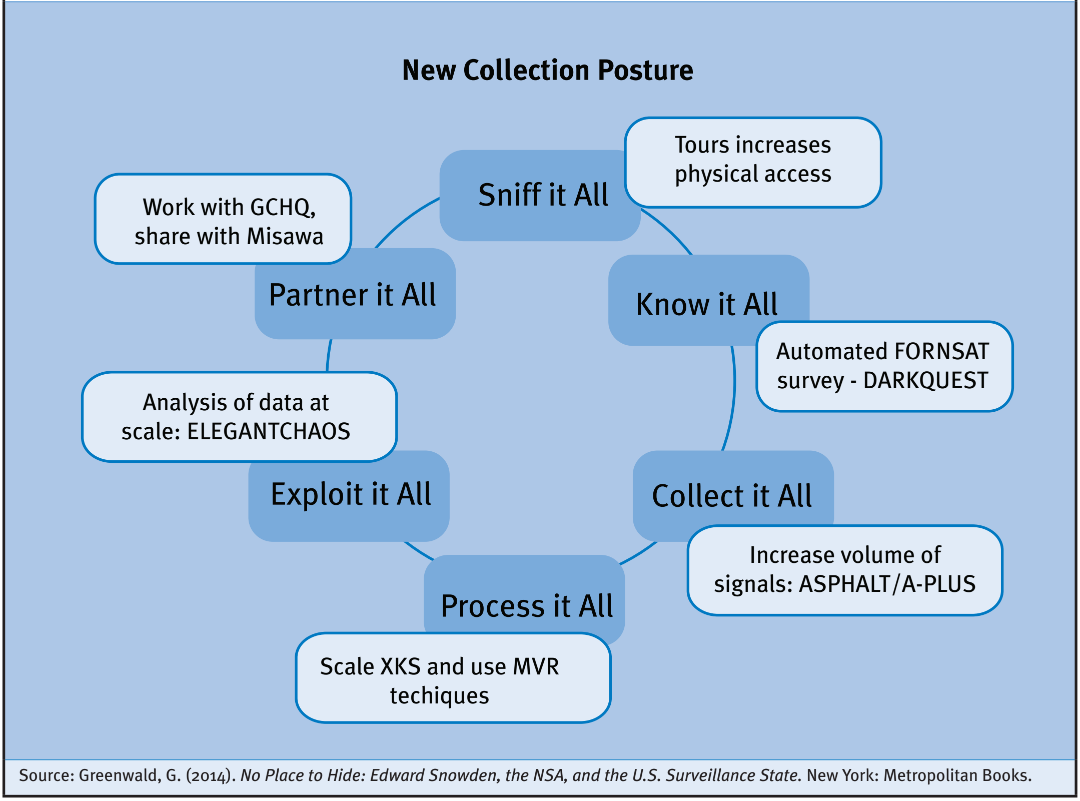
[32] Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York, Metropolitan Books, p. 97.

[33] Schneier, B. (2014). NSA Surveillance and What To Do About It. Presentation at the Stanford Center for Internet and Society, Stanford CA, USA, 22 April. https://youtube.com/watch?v=3v9t_IoOgyI

[34] Gellman, B., & Soltani, A. (2013, October 30). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post*. 30 www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

FIGURE 1.

The NSA's collection posture: A top slide from a secret presentation by the NSA to the annual conference of the Five Eyes


New Collection Posture

Sniff it All
Tours increases physical access
Know it All
Automated FORNSAT survey - DARKQUEST
Collect it All
Increase volume of signals: ASPHALT/A-PLUS
Process it All
Scale XKS and use MVR techiques
Exploit it All
Analysis of data at scale: ELEGANTCHAOS
Partner it All
Work with GCHQ, share with Misawa

Source: Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan Books.

that it could mostly have gotten through the PRISM programme. In addition to highlighting the NSA's massive institutional overreach and global privacy invasion, Snowden's disclosures also highlight the many points at which our data is insecure, and the vast numbers of vulnerabilities to surveillance that exist throughout our digital world. However, while the NSA is the largest threat in the surveillance game, it is not the only threat. Governments all around the world are using the internet to surveil their citizens. Considering the rate of technological change, it is not unforeseeable that the methods, tools and vulnerabilities used by the NSA will be the tools of states, cyber criminals and low-skilled hackers of the future. Regardless of who the perceived attacker or surveillance operative may be, and whether it is the NSA or not, large-scale, mass surveillance is a growing cyber security threat.

It has also been disclosed that the NSA and GCHQ have actively worked to make internet and technology users around the world less secure. The NSA has placed backdoors in routers running vital internet infrastructures.[35] The GCHQ has impersonated social networking websites like LinkedIn in order to target system administrators of internet service providers.[36] The NSA has been working with the GCHQ to hack into Google and Yahoo data centres.[37] The NSA also works to undermine encryption technologies, by covertly influencing the use of weak algorithms and random number generators in encryption products and standards.[38] The NSA in its own words is working under the BULLRUN programme to "insert vulnerabilities into commer-

[35] Gallagher, S. (2014, May 14). Photos of an NSA "upgrade" factory show Cisco router getting implant. *Ars Technica*. arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant

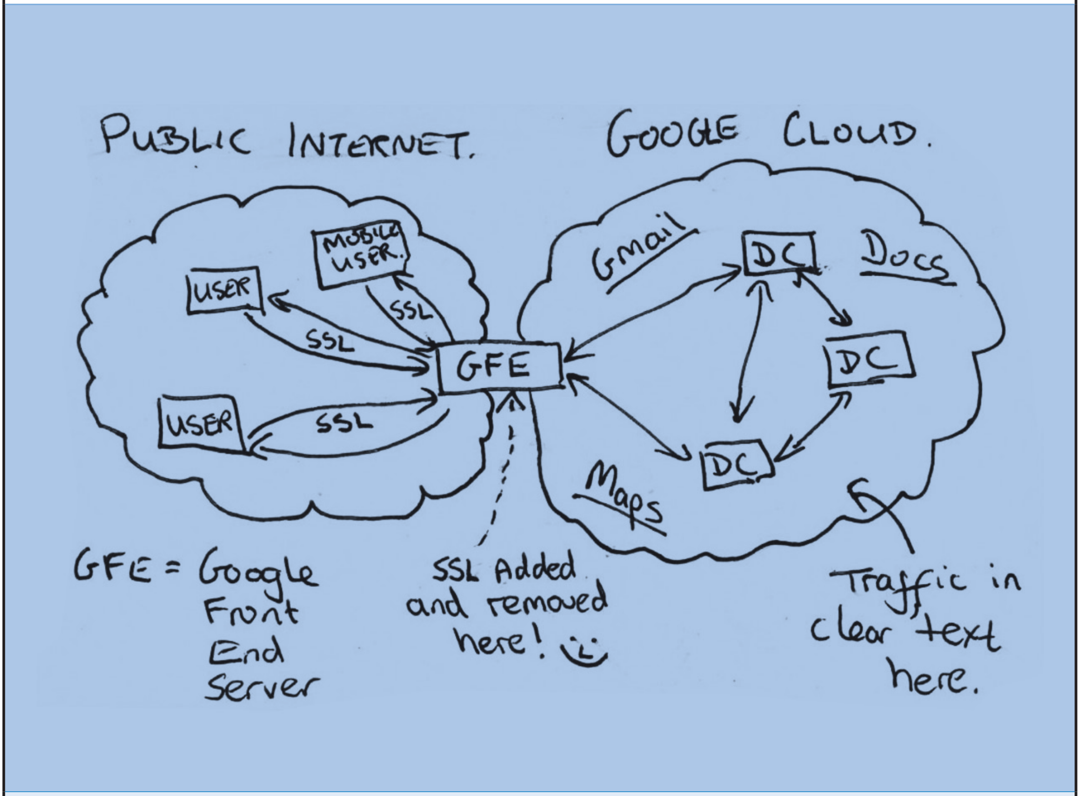
[36] Faviar, C. (2013, September 20). Snowden docs now show Britain, not NSA, targeted Belgian telco. *Ars Technica*. arstechnica.com/tech-policy/2013/09/snowden-docs-now-show-britain-targeted-belgian-telco-not-nsa

[37] Gellman, B., & Soltani, A. (2013, October 30). Op. cit.

[38] Guess, M. (2013, September 11). New York Times provides new details about NSA backdoor in crypto spec. *Ars Technica*. arstechnica.com/security/2013/09/new-york-times-provides-new-details-about-nsa-backdoor-in-crypto-spec

FIGURE 2.

This NSA slide demonstrates where Google's private cloud meets the public internet


PUBLIC INTERNET.
GOOGLE CLOUD.
MOBILE USER.
USER
USER
SSL
SSL
SSL
GFE
Gmail
DC
Docs
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here! ☺
Traffic in clear text here.

Source: Washington Post

cial encryption systems, IT systems, networks, and endpoint communications devices used by targets" and to "influence policies, standards and specifications for commercial [encryption] technologies."[39] The NSA is also believed to hoard knowledge about vulnerabilities rather than sharing them with developers, vendors and the general public,[40] as well as even maintaining a catalogue of these vulnerabilities for use in surveillance and cyber attacks.[41] None of these activities serve to make the internet more secure. In fact, they do the very opposite. As US Congresswoman Zoe Lofgren commented: "When any industry or organisation builds a backdoor to assist with electronic surveillance into their product, they put all of our data security at risk. If a backdoor is created for law enforcement purposes, it's only a matter of time before a hacker exploits it, in fact we have already seen it happen."[42]

The fact that the NSA is actively working to make the internet insecure points to the contradictions in its dual mandate: simultaneously securing and breaking cyber security. On the one hand it is tasked with securing information and communications networks (falling under its "Information Assurance" mandate), and on the other hand it is tasked with surveilling information and communications networks (its "Signals Intelligence" mandate).[43] Similar tensions exist within the US military, which

[39] New York Times. (2013, September 5). Secret Documents Reveal N.S.A. Campaign Against Encryption. *New York Times*. www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html

[40] Electronic Frontier Foundation. (2014, July 1). EFF Sues NSA, Director of National Intelligence for Zero Day Disclosure Process. *EFF*. https://www.eff.org/press/releases/eff-sues-nsa-director-national-intelligence-zero-day-disclosure-process

[41] Appelbaum, J., Horchert, J., & and Stöcker, C. (2013, September 29). Shopping for Spy Gear: Catalog Advertises NSA Toolbox. www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html

[42] National Insecurity Agency: How the NSA's Surveillance Programs Undermine Internet Security. Panel discussion at the New America Foundation, 8 July 2014. https://youtube.com/watch?v=K1ox5vwnJZA

[43] Ibid.

is tasked with both defending national networks from hacking attacks as well as with conducting offensive hacking attacks. The US "cyber command", the military command for the "cyber domain", is under the stewardship of the NSA commander. This conflict of interest in the NSA's dual role has not been addressed in current NSA reform. Tasked with "national security", intelligence agencies like the NSA have a conflicting mandate that cannot enable them to actually provide US citizens with cyber security, in the same way that states are for example able to provide us with physical security. It will always be against the interests of intelligence agencies to assure the provision of secure technologies that cannot be eavesdropped on. This is exacerbated by a cyber security-surveillance industrial complex of government agencies and private contractors selling hacking and surveillance products, with revolving doors between the two. We need to be very wary of intelligence agencies being given roles as stewards of cyber security.

Similarly, we cannot look to corporations for protection. Through mechanisms of intermediary liability, corporations are pressured by governments into cooperating with governments in surveillance programmes like PRISM, or the "Snoopers Charter" in the United Kingdom.[44] It would also not be within the interests of many tech companies to protect privacy and security to the extent that data is fully encrypted, not just during transit, but also in storage. Google's "Chief Internet Evangelist" Vint Cerf stated at the Internet Governance Forum in 2011 that this would not be in Google's interest, as "we couldn't run our system if everything in it were encrypted because then we wouldn't know which ads to show you."[45]

Recommendations

Civil society needs to articulate an agenda for cyber security that puts the security of human beings at the centre of the debate.

Making cyber security a national security issue can be counterproductive due to its potential for abuse. Cyber security also may be better dealt with by the technical community, the private sector and civil society. The state and military may not always be best suited to dealing with cyber security, and intelligence agencies may have a conflict of interest in ensuring cyber security.

Civil society needs to be wary of putting too much trust in either governments or corporations for assuring cyber security. Responsibility for cyber security should be distributed and not concentrate power too much in one particular place.[46]

Cyber security starts at home. Security is a collective effort that comes with collective responsibilities. If we are insecure, if we do not encrypt our communications, then those who we communicate with are also insecure. We therefore have a responsibility towards ourselves, but also towards others to secure our communications. All users should run modern operating systems and software that receive security updates, run an antivirus, and try to encrypt as much communications as possible.

Widespread use of encryption and privacy tools. Encryption protects communications from a multitude of cyber threats, including surveillance, theft and hacking. Encryption cannot fully protect us from surveillance, as it does not hide the metadata (for example, who the sender and recipient of the email are). Through metadata, a picture of our associations may be drawn, and anonymity tools provide another measure of protection from this. Edward Snowden's revelations have taught us that there are some tools that do work. PGP encryption is effective at encrypting email communications. The anonymity tool TOR, if used correctly, will work to anonymise communications and provide an extra layer of privacy on top of encryption. The lengths to which the NSA and GCHQ have gone (mostly unsuccessfully) to crack TOR is evidence of this. These tools can be complicated to use, but with a little training they are within the reach of many internet users.[47]

Encryption as resistance against mass surveillance. Encryption may not always work in the future, as quantum computers may decrypt our stored communications.[48] Snowden's revelations have also shown us how easy it is for intelligence agencies (like the NSA) to influence encryption

[44] Grice, A. (2014, July 11). Emergency data law: David Cameron plots to bring back snoopers' charter. *The Independent*. www.independent.co.uk/news/uk/emergency-data-law-government-railroading-through-legislation-on-internet-and-phone-records-9596695.html

[45] Soghoian, C. (2011, November 2). Two honest Google employees: our products don't protect your privacy. *Slight Paranoia*. paranoia.dubfire.net/2011/11/two-honest-google-employees-our.html

[46] Ron Deibert has made this argument in: Deibert, R. (2012). *Distributed Security as a Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace*. Calgary: Canadian Defence and Foreign Affairs Institute. www.cdfai.org/PDF/Distributed%20Security%20as%20Cyber%20Strategy.pdf

[47] Guidelines on securing oneself online are available at securityinabox.org, cryptoparty.org, or en.flossmanuals.net/basic-internet-security

[48] There are concerns around how encrypted information, captured and stored, could in the future be decrypted as quantum computing advances (ushering in an age of "post-quantum cryptography"); however, this is a long-term consideration. See: Arcieri, T. (2013, July 9). Imperfect Forward Secrecy: The Coming Cryptocalypse. *Tony Arcieri*. tonyarcieri.com/imperfect-forward-secrecy-the-coming-cryptocalypse

standards and implementation. Vulnerabilities in software will always allow cryptography and anonymisation tools to be bypassed,[49] and it is always easier to hack someone than to crack encryption. Widespread use of encryption, however, increases the cost of mass surveillance. It can be an effective way of containing and restricting mass surveillance, as it increases the cost to whomever is doing the spying, through the need for increased processing, capture and storage of data. Widespread use of encryption could force intelligence agencies like the NSA or GCHQ to focus on targeted interception, rather than bulk collection.[50] Encryption is becoming increasingly more widespread after Snowden's revelations. Yahoo, late to encryption, has finally turned on encryption as default for connections to its mail client. Both Google and Yahoo have begun encrypting internal links in their network. Widespread use of encryption and privacy tools does not just protect us from the NSA; they also help to mitigate a whole range of cyber security threats, from espionage to fraud to cyber attacks on activists and dissidents.

The wider use of up-to-date free/libre and open source software. The use of free/libre and open source software (FLOSS or FOSS) is another way in which we can increase our cyber security. FLOSS software is open source, which means that the source code is available for anyone to read. Vulnerabilities can be found more easily in open source code than they can in proprietary software. It is harder for malicious actors to purposively insert vulnerabilities ("backdoors") in FLOSS software. The example of Heartbleed has taught us that there are not always enough eyes reviewing security-critical software code, and that human investment in security-critical open source software and in open source code review is needed.

We have also identified a common use case which highlights the potential benefits of a shift to open source software: Windows XP. As Microsoft no longer provides security updates, XP users will be open to thousands of vulnerabilities, the quantity of which will only grow over time. The push to migrate users off this platform will continue, with governments/business (particularly in developing countries) increasingly adopting FLOSS as an alternative.[51] GNU/Linux, a FLOSS operating system, can run on old computers and still receive security updates, which are free of charge and shared between new and old systems. GNU/Linux allows for security updates that are mainly software based, and can mitigate the need for buying new hardware.

More explicit focus needs to be placed on vulnerabilities in cyber security discourse. Security researchers need to be incentivised to disclose vulnerabilities in software and hardware to the vendors involved or the users infected, rather than selling this information to intelligence agencies, cyber criminals and other malicious actors. An example of positive incentivisation may be "bug bounty" programmes, which reward security researchers with fame, recognition and money for finding and disclosing vulnerabilities to the software vendors involved. Microsoft, Google, Twitter and many other big-tech companies are starting to employ such programmes. As malicious actors may always offer more money for vulnerabilities, it may be necessary to investigate regulating the market in zero-days.[52] This should be done carefully, however, without criminalising security researchers and putting them at risk for doing beneficial work.

It is also essential for governments and civil society to also be concerned with forever-day vulnerabilities. The use of Windows XP should immediately cease, and industrial control systems controlling national infrastructures like power grids should be immediately migrated to systems receiving modern security updates, or firewalled or air-gapped from the internet.

Cyber security is augmented by strong data protection rules. These rules should include requirements that companies or organisations encrypt and secure data, should regulate the sharing of data with third parties, and should have requirements that companies inform clients and customers when there are data breaches that have affected their security.

Information sharing. The proposed Cybersecurity Information Sharing Act (CISA) in the US requires private sector companies to hand over information about cyber threats to the Department of Homeland Security: According to *The Guardian:*

[49] At the time of writing, researchers have revealed that there are serious vulnerabilities in the TOR, I2P and TAILS anonymisation tools, but have not revealed the details. Regarding TOR, this is because of legal concerns, and regarding I2P and TAILS, the researcher has not fully disclosed the details.

[50] Schneier, B. (2014, February 10). NSA Surveillance and What To Do About It. Presentation at MIT, Cambridge MA, USA, 10 February. bigdata.csail.mit.edu/node/154

[51] See en.wikipedia.org/wiki/List_of_Linux_adopters for a list of organisations who have moved over to Linux, an open source operating system.

[52] A proposal for such regulation is outlined in Gaycken, S., & Lindner, F. (2012). Zero-Day Governance: an (inexpensive) solution to the cyber security problem. Paper submitted to Cyber Dialogue 2012: What Is Stewardship in Cyberspace?, Toronto, Canada, 18-19 March. www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012papers/CyberDialogue2012_ga-ycken-lindner.pdf

It is written so broadly it would allow companies to hand over huge swaths of your data – including emails and other communications records – to the government with no legal process whatsoever. It would hand intelligence agencies another legal authority to potentially secretly re-interpret and exploit in private to carry out even more surveillance on the American public and citizens around the world. And even if you find out a company violated your privacy by handing over personal information it shouldn't have, it would have immunity from lawsuits – as long as it acted in "good faith". It could amount to what many are calling a "backdoor wiretap", where your personal information could end up being used for all sorts of purposes that have nothing to do with cybersecurity.

Information sharing, while infringing our privacy, is also a threat to cyber security: as more information is shared with third parties, it becomes harder to secure. Furthermore, surveillance is not a solution to the problems of cyber security, as this report has shown. If we want to meaningfully talk about interventions in information sharing and cyber security, then we should talk about vulnerabilities. Rather than information about "threats" or about the personal lives of internet users being shared, information about vulnerabilities that affect our security need to be shared with all stakeholders – governments, developers, vendors and internet users – in a responsible manner, so that this information cannot be hoarded and used to weaken all of our cyber security.