APC ISSUE PAPERS

A CYBER SECURITY AGENDA FOR CIVIL SOCIETY: WHAT IS AT STAKE?

Alex Comninos

INTRODUCTION

The security of digital networks and of networked digital information is increasingly important to stakeholders in governments, the private sector and civil society. Cybercrime is increasing in sophistication.[1] States are accusing each other of hacking incidents.[2] Civil society organisations, states, corporations, and internet users are exposed and become victim of viruses and malware, data breaches, online privacy violations, and surveillance. Governments and corporations are spying on netizens, human rights defenders (HRDs) especially are becoming victims of such surveillance. "Hacktivism" is emerging as a form of protest often in defense of human rights, but may also possibly infringe on rights, or trigger government responses that infringe on these rights.[3] Women human rights defend-

[1] RSA 2012 Cybercrime Trends Report: The Current State of Cybercrime and What to Expect in 2012, http://www.rsa.com/products/consumer/whitepapers/11634_CYBRC12_WP_0112.pdf

[2] US and China accuse each other of cyber warfare, Russia Today 19 February 2009, http://rt.com/usa/cyber-china-war-unit-604/

[3] James Ball "By criminalising online dissent we put democracy in peril", The Guardian 1 August 2011, http://guardian.co.uk/commentisfree/2011/aug/01/onlinedissent-democracy-hacking; Cory Doctorow, Pirate Bay to Anonymous: DDoS is censorship, cut it out, BoingBoing 1 May 2012, http://boingboing.net/2012/05/11/pirate-bay-to-anonymous-ddos.html, Jay Leiderman, Justice for the PayPal WikiLeaks protesters: why DDoS is free speech, The Guardian January 22 2013, http://www.guardian.co.uk/commentisfree/2013/jan/22/paypal-wikileaks-protesters-ddos-free-speech

Alex Comninos is a scholar and researcher on the internet and information and communications technologies from a human rights perspective. He is a DAAD scholar and doctoral student in the Department of Geography, Justus Liebig University Gießen, Germany. He has an MSocSci in International Relations from the University of Cape Town.

APC
ASSOCIATION
FOR PROGRESSIVE
COMMUNICATIONS

ers (WHRDs), important stakeholders in cyber security, face surveillance, information security vulnerabilities, and information security compromises that can be life threatening. At the same time, ICTs - which need to be secure - can be used by WHRDs to report on and defend themselves against human rights abuses.[4]

National security is being used by governments as a justification to censor, control or surveil internet use, and sometimes to shut down communications. Some cyber security specialists in the military are establishing cyber units, and an escalating arms race in cyberspace is emerging,[5] accompanied by the growth of a "cyber-industrial complex."

The private sector is increasingly involved in internet control. Through mechanisms of intermediary liability, telecommunication companies, internet service providers (ISPs) and other private sector actors now actively police the internet."[6]

While governments, militaries, intelligence agencies and the private sector are taking the lead in steering cyber security debate and policies, civil society needs to engage in cyber security on an equal footing. Robert Deibert has argued that civil society is "increasingly recognised as an important stakeholder in cyberspace governance" and needs to develop a cyber security strategy "that addresses the very real threats that plague governments and corporations, addresses national concerns in a forthright manner, while protecting and preserving open networks of information and communication."[7]

This paper introduces some important conceptual issues in cyber security; investigates some important cyber security threats, and provides suggestions on what a civil society approach to cyber security should look like.

[4] Danna Ingleton, Let's stop our fear of tech leading to misuse of security legislation, in Crossing borders : cyberspace and national security, GenderIT, 25 October 2012, http://www.genderit.org/node/3684.

[5] Ron Deibert, Towards a cyber security strategy for civil society, in Alan Finlay (ed.) *Global Information Society Watch 2011: Internet rights and democratization,* APC & HIVOS, http://www.giswatch.org/en/freedom-expression/towards-cyber-security-strategy-global-civil-society

[6] Ibid.

[7] Ibid.

CONCEPTUALISING CYBER SECURITY

Definition

Cyber security refers to the security of digital information stored on electronic networks, as well as the security of the networks that store and transmit information. However there is little consensus on how exactly it is defined. *Cyber security* is sometimes used interchangeably with *information security* – "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."[8] Information security and cyber security refer generally to the same thing. However, information security is used by organisations and IT professionals, while cyber security is more generally used in policy debates, and when information security issues are framed as national security issues.

The International Telecommunications Union (ITU) defines cyber security as:

> "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets[9] ... Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation [and] Confidentiality."[10]

This definition is somewhat broader than information security. Rather than just protecting information systems, it also protects, "cyber environment" (a rather vague term) and "user's assets". It refers to not just the *securing of information systems,* but also to the *use of information systems to secure assets.*

So how broad should the concept of cyber security be? Which issues should be included, and which issues should not? An OECD[11] report states that cyber security "has come to mean a huge spectrum of things. Not only does this lead to powers that are overly broad in scope and application, but it also risks generating a consensus that is illusory,"[12] including the risk of too many issues resulting in the concept losing its coherence. The broader the concept of cyber security is, the more issues it puts on the agenda of states' military and intelligence agencies. Many issues, while relying on the secure use of information and communication technologies (ICTs) and the internet, may not be best addressed by national security, or even information security frameworks, or by state or military solutions. It is not always helpful to discuss something as a cyber security issue, even if it has obvious information security dimensions.

Securitisation

When issues are discussed as security issues, they are given a sense of urgency and importance. Talking about an issue as security issue often involves presenting a threat to a society's way of life, and justifying extraordinary or emergency measures to counter the threat. When issues are transformed, through speech into national security issues, this is called securitisation. Securitisation involves "the designation of an existential threat requiring emergency action, or special measures, and the acceptance of that specific delegation by a significant audience."[13] When issues are securitised successfully, they become national security issues and the manner in which they are dealt with

[8] Integrity "means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;" confidentiality "means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information" and availability "means ensuring timely and reliable access to and use of information." Richard Kissel, *Glossary of Key Information Security Terms,* National Institute of Science and Technology, US Department of Commerce February 2011 *p. 93.* http://books.google.com/books?id=k5H3NsBXIsMC

[9] "Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment."

[10] International Telecommunications Union, Telecommunications Standardization Sector, Overview of Cyber security, Recommendation ITU-T X.1205 (04/2008), http://www.itu.int/ITU-T/recommendations/rec.aspx?id=9136 Adopted by ITU Resolution 181, Guadalajara, 2010, http://www.itu.int/osg/csd/cyber security/WSIS/RESOLUTION_181.pdf

[11] Organisation for Economic Cooperation and Development (OECD).

[12] OECD (2012), "Non-governmental Perspectives on a New Generation of National Cyber security Strategies", OECD Digital Economy Papers, No. 212, OECD Publishing, http://dx.doi.org/10.1787/5k8zq92sx138-en, p 6.

[13] Barry Buzan, Ole Waever & Jaap de Wilde, 1998, *Security: a new framework for analysis,* Lynne Rienner: Boulder, Colorado, p. 27.

is changed "beyond the established rules of the game". The issue is framed "either as a special kind of politics or as above politics."[14] A successful securitisation has three components: presenting an issue as a threat, emergency action to deal with the threat, and effects on stakeholder relations by changing how the issue is normally dealt with.[15]

The securitisation of cyberspace is an important factor shaping the global communications ecosystem. Issues regarding information security, the internet, internet governance, and other areas, are through the lens of cyber security being securitised and transformed into national security issues. This negatively affects the existing governance structures and decision mechanisms around these issues. When an issue is securitised it does not necessarily enhance civil society's voice and role as a stakeholder in the governance of that issue. When extraordinary or emergency actions are called for, we must make sure that these measures do not have negative consequences affecting the openness and security of the internet, and do not have negative human rights consequences.

A historical perspective: the widening and deepening of the concept of security

The history of the concept of security contains some lessons that can be applied to cyber security. Over the last three decades, the concept of security as well as state security agenda have widened to include many sectors and issues. In the context of *detente* and the end of the Cold War academic and policy debates began between "*wideners*", those who argued for widening the definition and agenda of security beyond the security of the states and strategic cold war issues; and "*narrowers*", those who wanted to keep the narrow definition and agenda of security, focusing on military issues and the security of the state. Since the end of the cold war, governments, the military, academia, and civil society have participated in the widening of the concept of security to include other sectors, not traditionally related to state security, for example, cultural security, economic security, environmental security, climate security, and food security. At the same time the concept has been "deepened" to include humans as the central object of security, rather than states or militaries.

The post-cold war concept of security is now "very broad... still contains the problem of being very broad" it is "even more abstract than before" and is still a concept that "is in the hands of the state" and can be used against people.[16] With a wider definition of security, governments now have more excuses for deploying the coercive apparatus of the state, or for implementing extraordinary measures – like surveillance and regulation of an increasing number of issues. Many issues that civil society should deal with have been brought on the national security agenda of states, often giving the state more power to intervene in these issues.

The concept of cyber security is currently undergoing a similar deepening and widening. Cyber security and information security were previously technical concepts, discussed mainly by geeks, IT professionals, corporations, states, and military, intelligence and security agencies. The concepts are now increasingly important to us all and have expanded to include more than the previously narrow concerns of the technical community, business and the state. This gives more stakeholders opportunities to engage in cyber security. However, accompanying this process contributes to widening the cyber security agenda. This widened agenda can result in other issue areas in internet governance, global governance, national governance, policy legislation and regulation being brought onto the cyber security agenda and thus national security agenda of states. This can result in issues being moved away from current governance structures dealt with through multi-stakeholder approaches. Civil society may be marginalised as a result of this. As civil society, we must make sure that we can harness the widening of the concept of cyber security without marginalising our role as stakeholders. When we talk about cyber security, what is at stake is the voice and power of civil society as a stakeholder.

[14] Ibid, p. 24.

[15] Ibid.

[16] See "A Conversation with Annette Seegers" and for a longer explanation see, Annette Seegers, "The New Security in a Democratic South Africa", presentation at The Robert Strauss Center for International Security and Law", November 1 2010, http://blip.tv/robert-strauss-center/the-new-security-in-democratic-south-africa-4362239. Based on this paper Seegers, Annette (2010) 'The new security in democratic South Africa: a cautionary tale', Conflict, Security & Development, 10: 2, 263 — 285.

ISSUES TO CONSIDER

It is far beyond the ambit of this paper to provide a comprehensive outline of all relevant cyber security threats. The aim of the paper is rather to encourage critical thinking about cyber security, and raise some issues in order to help civil society in developing cyber security strategies. A few thematic and important issues with regards to cyber security will be discussed below, before moving to the recommendations.

Techno-speak and fear mongering

Cyber security can be quite complex to netizens without a technical background. This can lead many people, including the media, policy makers, and stakeholders from government, business and civil society, to take reports at face value. Cyber security issues may easily be misinterpreted, misunderstood, misrepresented or misreported. Due to the relative anonymity afforded by the internet, it is hard to attribute responsibility or causation for cyber attacks and cyber incidents. In this environment, unsubstantiated claims can spread quickly through policy debates.

Many inaccurate stories about cyber security incidents are repeated over and over again, although often they lack evidence of any depth further than mere speculation. US President Barack Obama has, for example, said: "We know that cyber intruders have probed our electrical grid, and that in other countries cyber attacks have plunged entire cities into darkness"[17] – although he did not mention which country this occurred in. The US media picked up on the story, with the popular TV programme *60 Minutes* claiming that "[s]everal prominent intelligence sources confirmed that there were a series of cyber attacks in Brazil" in 2005 and 2007.[18] These allegations are still repeated by the media without substantiation. A Wikileaks cable and a statement by the Brazilian electricity regulator claim the blackouts were not the result of cyber attacks, but were rather caused by "pollution in the chain of insulators due to deposits of soot".[19]

Militarisation of cyberspace and a cyber arms race

Cyber security is being increasingly brought onto the security agenda of states. States around the world are beginning to establish within their militaries "cyber commands" or cyber units. The US Cyber Command has had "operational capacity" since May 2010. "Cyber commands" are becoming an attractive idea to other states. The defence secretary in the UK has proposed an integrated cyber command under the Ministry of Defence. The Indian Ministry of Defence is looking to establish a "Cyber Control and Command Authority". China has established a "Blue Army" to defend the People's Liberation Army from attacks on its networks.[20] Iran also has plans to establish a cyber command for the countries armed forces.[21] Cyber units are used to crush online dissent. In March 2011, in a meeting of the ruling party of Sudan's "cyber battalion", the party announced that the party's "cyber jihadists" would "crush" online dissidents calling for regime change.[22] Cyber units are also deployed in conflict zones, such in Syria, where supporters of the government have established the "Syrian Electronic Army" which is used to surveil activists and members of the Free Syrian Army.[23] "Others are adopting less conventional means, including providing tacit support

[17] Cyberwar: Sabotaging the System, CBS News, June 15th 2010, http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml see the 60 Minutes segment at https://www.youtube.com/watch?v=IPHHd8YW9EA (part 1) and https://www.youtube.com/watch?v=dU2XPFoyAR8 (part 2).

[18] Ibid.

[19] Marcello Soares, Brazilian Blackout Traced to Sooty Insulators, Not Hackers, *Wired Magazine* 11 November 2009, http://www.wired.com/threatlevel/2009/11/brazil_blackout/. Brian Krebs, Cable: No Cyber Attack in Brazilian '09 Blackout, Krebs on Security 03 December 2010, http://krebsonsecurity.com/2010/12/cable-no-cyber-attack-in-brazilian-09-blackout/

[20] Alex Comninos, "Anonymous: Information Conflict and New Challenges to Peace Practitioners", Peace Magazine 27(4), October 2011, http://peacemagazine.org/archive/v27n4p16.htm

[21] Iran to launch first cyber command, Press TV, June 15 2011, http://presstv.com/detail/184774.html

[22] Sudan's NCP says its "cyber-Jihadists" ready to "crush" online oppositionists, Sudan Tribune, March 22 2011, http://www.sudantribune.com/Sudan-s-NCP-says-its-cyber,38372

[23] "What is the Syrian Electronic Army?", Mashable, August 12 2012, http://mashable.com/2012/08/10/syrian-electronic-army/

for pro-patriotic groups to engage in offensive cyber attacks in defence of the state, as seems to be the case in Iran, Syria, Russia, Burma and China."[24]

States are allocating increasing resources to information security, as well as to information warfare. In 2011, while the US faced a budget crisis, the Pentagon requested USD 3.2-billion worth of funding be allocated to cyber security —a figure roughly equal to the military expenditure of Morocco or Argentina in that year.[25] Increased military spending on cyber warfare is arguably a waste of resources, as well as not necessarily the right solution to cyber security problems.

The internet is becoming increasingly militarised. Viruses, once the tools of cybercriminals and the occasional prankster, are now being actively developed by military and intelligence agencies. The Stuxnet virus, responsible for the sabotaging of centrifuges involved in the Iranian uranium enrichment programme was the first widespread malware specifically designed to infect industrial equipment. Stuxnet was possibly designed and deployed with the backing of state intelligence and security agencies (allegedly the US and Israel).[26] Cofer Black, ex-Director of the CIA's Counterterrorism Center (and director of a subsidiary of the largest private security contractor to the US State Department) announced at the 2011 Black Hat, an information security conference, that Stuxnet marked the "Rubicon of our future."[27] Whether or not this represents an historical turning point (or an implicit admission of involvement by a US agency in Stuxnet), this highlights the military industrial complex's tacit acceptance of malware as a tool to be used by states in future information conflicts.

Since the emergence of Stuxnet, there have been reports of another virus, the Flame virus, which has spread through a number of countries in the Middle East and North Africa using the Stuxnet code. In addition to this, the Stuxnet source code is now available on the internet, allowing a multitude of actors to adapt the code for their own purposes.

The Defence Ministry of Japan has commissioned Fujitsu to develop for them a "defensive virus" for USD 2.3 million, and which has "the ability to identify the source of a cyber attack with a high level of accuracy, then replicate itself from computer to computer, cleaning up viruses across the network." However, according to a security expert, the virus "could have unintended consequences, such as being difficult to control". An "out-of-control 'good' virus could spread randomly or unexpectedly" making it hard to contain.[28] The virus, spreading outside of Japan would also possibly infringe on sovereignty of other countries, possibly sparking conflict.

The cyber security industrial complex

> *"In the councils of government, we must guard against the acquisition of unwarranted influence, whether sought or unsought, by the military-industrial complex. The potential for the disastrous rise of misplaced power exists and will persist.*
> *We must never let the weight of this combination endanger our liberties or democratic processes. We should take nothing for granted. Only an alert and knowledgeable citizenry can compel the proper meshing of the huge industrial and military machinery of defense with our peaceful methods and goals, so that security and liberty may prosper together."*
>
> - DWIGHT D. EISENHOWER, President of the United States of America, Farewell Address to the Nation, 1961[29]

Another important threat with regards to cyber security is the emergence of a cyber-industrial complex. Modern militaries have highly developed business networks with suppliers of defence equipment and contractors of defence services. Often, staffs of defence companies are ex-government officials, and there exists a "revolving door" between the two. Both have a vested interest in

[24] Deibert, op. cit.

[25] Alex Comninos, "Anonymous: Information Conflict and New Challenges to Peace Practitioners", op. cit.

[26] Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History", Wired, July 11 2011, http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/

[27] Tabassum Zakaria, "Former CIA official sees terrorism-cyber parallels", Reuters, 3 August 2011, http://www.reuters.com/article/2011/08/03/us-usa-security-cyber-idUSTRE7727AJ20110803; and Glenn Chapman, "Cold War gives way to Code War: CIA veteran", Agence France Presse, 4 August 2011, http://www.google.com/hostednews/afp/article/ALeqM5h-_86Ftav0uDHvMYDzydPgVWjNzQ?docId=CNG.0dcc70d787af82f2b283aeb2af9d940e.e01

[28] Gerry Smith, Fujitsu Cyberweapon Developed In Japan: 'Good' Virus Created For Cyber Defense, Huff Post Tech 04 January 2012, http://www.huffingtonpost.com/2012/01/04/fujitsu-cyberweapon-japan_n_1183462.html. See also Graham Cluley, Why Japan's search-and-destroy cyber weapon could be a very bad idea, Naked Security January 12 2012, http://nakedsecurity.sophos.com/2012/01/03/japan-cyber-weapon-bad/

[29] Text at: http://coursesa.matrix.msu.edu/~hst306/documents/indust.html, Video at: http://www.youtube.com/watch?v=8y06NSBBRtY

increased defence budgets, and in order to justify these budgets they have to present threats to their citizenry, parliaments and governments. The military industrial complex is always looking for new threats in order to justify new spending, and the emerging "cyber threat" provides one such opportunity. The cyber-industrial complex is not just developing offensive and defensive cyber weapons, but also increasingly developing surveillance equipment, a new industry is emerging that "secretly vacuums up the data and preserves it forever on high-end servers that hold many petabytes (a million gigabytes) of information". This new industry "offers new tools to search that data and reconstruct our past, and even our real-time movements via our mobile phones, in a way that could well come back to haunt us."[30]

[30] Pratap Chatterjee, The new cyber-industrial complex spying on us, *The Guardian* 2 December 2011, http://www.guardian.co.uk/commentisfree/cifamerica/2011/dec/02/cyber-industrial-complex-spying.

CYBER SECURITY AND CENSORSHIP

Cyber security can be used to introduce and legitimise modes of censorship and normalise such censorship. In Russia, for example, a "Single registry" of banned websites is intended to give the government the ability to shut down any website that is deemed as harmful to children; including sites containing child pornography, information about drugs, and information on how to commit suicide. The registry "however could lead to random censorship of websites and free speech,"[31] and "wind up blocking all kinds of online political speech" and "thanks to the spread of new internet-monitoring technologies, the Register could well become a tool for spying on millions of Russians."[32]

The role of intelligence agencies

Here lies a fundamental conflict of interest when it comes to cyber security. Intelligence agencies may like to secure their own infrastructures, but if they wish to surveil others, they do not necessarily wish them to have secure information infrastructures. Secure and private channels of communication offer much fewer opportunities for intelligence gathering and surveillance than do insecure infrastructures. This means we need to be sceptical when intelligence agencies are involved in cyber security, and we must ensure that their operations are subject to civilian and parliamentary oversight. Civil society and lawmakers need to be especially vigilant in this regard.

Cyber security and surveillance

Cyber security should strive to protect netizens from surveillance. However, cyber security initiatives may give companies and governments more power to spy on users. For example, the proposed Cybersecurity Bill of 2012 in the USA would have "granted companies new powers to spy on users, to share that information with the government, and to claim broad legal immunity for their actions."[33] The second iteration of the Cyber Intelligence Sharing and Protection Act now before the House of Representative in the USA would provide a "cyber security" exception that overrides existing privacy laws. Companies would receive broad immunity for sharing information including the private communications of users with government agencies, in the name of cyber security. Corporations would be given free reign to collect and share "cybersecurity information" including personal information, with the only limitation that the information is collected for a "cybersecurity purpose."[34]

New social media threats

The growth of the cyber industrial complex, along with the growth of our online presence in social networks and on social media, has greatly augmented the surveillance capacities of intelligence agencies. For example, in 2009, the USA Central Intelligence Agency invested in a company that specialises in monitoring social media. The company, called Visible, "crawls over half a million web 2.0 sites a day, scraping more than a million posts and conversations taking place on blogs, online forums, Flickr, YouTube, Twitter and Amazon".[35]

In addition to potentially exposing civil society to surveillance, social media can also potentially expose civil society to manipulation. Cyber security firms have developed software that creates fake personas on social networks for the purpose of surveillance, as well as for manipulating online conversations to mimic the appearance of grassroots movements, a practice called "astroturfing". For example, in 2010 the US Air Force requested proposals for the development of astroturfing

[31] Bryan Bishop, Internet censorship bill passes upper house of Russian Parliament, The Verge July 18 2012, http://www.theverge.com/2012/7/18/3168011/internet-censorship-bill-passes-upper-house-russian-parliament

[32] Andrei Soldatov & Irina Borogan, The Kremlin's New Internet Surveillance Plan Goes Live Today, *Wired* November 1 2012, http://www.wired.com/dangerroom/2012/11/russia-surveillance/all/

[33] Mark M. Jaycox, The Cyber security Act was a surveillance bill in disguise, *The Guardian* 2 August 2012.

[34] Mark M. Jaycox, CISPA, the Privacy-Invading Cyber security Spying Bill, is Back in Congress, Electronic Frontier Foundation 13 February 2013, https://www.eff.org/deeplinks/2013/02/cispa-privacy-invading-cyber security-spying-bill-back-congress.

[35] Noah Schachtman, U.S. Spies Buy Stake in Firm That Monitors Blogs, Tweets, *Wired Magazine* 19 October 2009, http://www.wired.com/dangerroom/2009/10/exclusive-us-spies-buy-stake-in-twitter-blog-monitoring-firm/

software – or "persona management" software – that would allow for the control of fake personas on social media platforms.[36]

Astroturfing software could be used to both surveil, as well as to spread propaganda, which is made to appear as if it legitimately comes from civil society. This comprises a serious information security threat (information security as mentioned above is about protecting the "confidentiality, integrity, and availability" of information and communications.) Journalist George Monbiot has commented that "[s]oftware like this has the potential to destroy the internet as a forum for constructive debate. It makes a mockery of online democracy."[37]

Software security: *Zero days* and *forever days*

Articles about cyber security are generally quite exciting (or terrifying). But the real challenge to cyber security however does not involve international terrorism, state sponsored espionage, or hackers on steroids. The problem lies in the source code of the software we use every day, whether this is the operating systems we use, the "apps" we run on our computing devices, our web browsers and the add-ons that make them run (e.g. Flash and Java), and the software used to build the websites that populate the internet. The real cyber security problem lies in *software security*. It is generally understood that the internet (the TCP/IP protocol) and the web were not designed to be secure. The internet was originally an academic network of trusted peers. Problems of trust and security were not of importance then and were not primarily addressed. While there has been progress in securing infrastructures (the development of Domain Name System Security Extensions (DNSSEC)[38] and the HTTPS protocol[39] for example), it is generally accepted that the internet cannot be redesigned for security, and that such a redesign would pose challenges to its interoperability. On top of the open internet infrastructures layer, exists the application layer. These are the applications which exist locally on our machines, in software which facilitates access to web and internet services, like web browsers, instant messaging and VoIP clients (e.g., Skype), as well as the software which drives the online services and web sites on which we store our data. It is in this layer in which security can be built in by design, but it is also in this layer in which there is the most insecurity. It is also in this layer that we are able to most easily implement fixes that can ensure the security of our information.

Expertise in fixing security bugs in code is improving but not keeping up with the pace of the growth of new bugs. Compared to 15 years ago, all popular and contemporary desktop operating systems (Windows, Linux and Mac) offer regular automated security updates for security "bugs" which are then "patched" by the updates. While we are finding more bugs in code, and viruses than ever before, we are getting better at finding them. At the same time we keep producing more and more code (computer and online applications) thus the net number of bugs, and thus security vulnerabilities in our code is increasing, resulting in more software bugs than ever before.[40]

A security bug (also called a vulnerability) is essentially a piece of software code, that does not take account of security, and can thus be exploited by people to gain access to data that they should not be able to under

[36] John Hudson, The Embarrassing Revelations of Cyber Security Firm HBGary Federal, The Atlantic Wire, February 24 2011, http://www.theatlanticwire.com/technology/2011/02/the-embarrassing-revelations-of-cyber-security-firm-hbgary-federal/20977; Happy Rockefeller, The HB Gary Email That Should Concern Us All, The Daily Kos 16 February 2011, http://www.dailykos.com/story/2011/02/16/945768/-UPDATED-The-HB-Gary-Email-That-Should-Concern-Us-All, the original request for proposal "Persona Management Software" (Solicitation number: RTB220610 22 June 2010) was for a "Online Persona Management Service. 50 User Licenses, 10 Personas per user." The "Software will allow 10 personas per user, replete with background, history, supporting details, and cyber presences that are technically, culturally and geographically consistent. Individual applications will enable an operator to exercise a number of different online personas from the same workstation and without fear of being discovered by sophisticated adversaries. Personas must be able to appear to originate in nearly any part of the world and can interact through conventional online services and social media platforms. The service includes a user friendly application environment to maximise the user's situational awareness by displaying real-time local information." Originally appearing at FedBizOpps.gov, archived at: http://www.seankerrigan.com/docs/PersonaManagementSoftware.pdf

[37] Ibid.

[38] DNSSEC are a set of Internet Engineering Task force specifications that add extensions to the DNS service that add data origin authentication and data integrity to the Domain Name System. It does not however not provide for confidentiality. See Arends et al., Request For Comment 4033, DNS Security Introduction and Requirements, March 2005, Internet Engineering Task Force, http://tools.ietf.org/html///rfc4033; See also RFCs 4034, and 4035, and http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions for a thorough explanation.

[39] The Hypertext Transfer Protocol Secure (HTTPS) adds some security to the Hypertext Transfer Protocol (HTTP) by adding bidirectional encryption between the user and the website, http://en.wikipedia.org/wiki/HTTP_Secure

[40] Gary McGraw, Cyber War, Cyber Peace, Stones, and Glass Houses, talk at Institute for Security, Technology, and Society (ISTS), Dartmouth College, 26 April 2012, http://www.ists.dartmouth.edu/events/abstract-mcgraw.html, http://www.youtube.com/watch?v=LCULzMa7iqs

normal circumstances. When a bug is discovered, a malicious hacker may make an "exploit", in order to compromise data or access to a computer. Malware – viruses and Trojan horses – are exploits that take advantage of these bugs. There are two important types of software bugs that are very relevant to cyber security. Dealing with them may be the most effective way of securing cyberspace: they are *zero-days* and *forever-days.*

Zero days are bugs/vulnerabilities, which have been discovered, unbeknownst to the original software developers. The original suppliers of the software are unable to patch the software as they may not be aware of its existence, or have not had time to fix the bug. They have had "zero days" to fix the vulnerability. A zero-day attack is an attack that takes advantage of a zero day vulnerability. They are particularly dangerous, as most people - other than security researchers or those with malicious intent, are unaware of the vulnerability, and are thus unable to protect themselves against these attacks. The most serious cyber security attacks come from zero day bugs and zero day exploits. The right thing to do when finding a zero day is to notify the original software developer, so that they may find a fix for the vulnerability. Furthermore, at some stage, users of the affected software that are rendered vulnerable must be informed, as well as perhaps other stakeholders and the public in general. "Like most technologies, the 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."[41] A recent article by *Forbes*, highlights a growing market for zero days that operate in a grey and unregulated manner. "Some legitimate companies operate in a legal grey zone within the zero-day market, selling exploits to governments and law enforcement agencies in countries across the world... But because sales are unregulated, there are concerns that some grey market companies are supplying to rogue foreign regimes that may use exploits as part of malicious targeted attacks against other countries or opponents. There is also an anarchic black market that exists… where exploits are sold to a variety of actors often for criminal purposes" and "there are fears that the burgeoning trade in finding and selling exploits is spiralling out of control, spurring calls for new laws to rein in the murky trade."[42] It is important to consider regulation when it comes to zero days. Software companies must be encouraged to find and fix zero-days in their own software, security researchers should also be incentivised to find zero days and notify companies and other stakeholders.[43]

A serious problem for cyber security for the average user, as well as for critical infrastructures connected to the internet, are "forever-days", "infinite-days" or "iDays". These "refer to bugs that never get fixed or take a long time to get fixed —even when they're acknowledged by the company that developed the software". While these bugs can affect everyday web users, they can also affect critical infrastructures, like industrial control systems, used often to control infrastructures such as power grids. Industrial control systems require large investments in equipment that is supposed to last years. Unlike the software development business cycle, operators of industrial control systems often cannot afford to update their systems regularly. There are for example well-documented vulnerabilities ("forever-days") in Siemens controllers that allowed for the Stuxnet virus to infect the Natanz nuclear reactors in Iran. These controllers also operate a vast array of machinery for different applications all over the world "used in nuclear facilities and other critical infrastructures, as well as in commercial manufacturing plants that make everything from pharmaceuticals to automobiles."[44]

[41] Ryan Gallagher, Cyberwar's gray market, Slate 16 January 2013, http://www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html; See also, Andy Greenberg, Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees), Forbes 21 March 2012, http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/

[42] Ryan Gallagher, Cyberwar's gray market, op. cit.

[43] A proposal for such regulation is outlined in Sandro Gaycken & Felix FX Lindner, Zero-Day Governance: an (inexpensive) solution to the cyber security problem, Paper submitted to Cyber Dialogue 2012: What is stewardship in cyberspace?, March 2012, http://www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012papers/CyberDialogue2012_gaycken-lindner.pdf

[44] Kim Zetter, Serious security holes found in Siemens control systems targeted by Stuxnet, Ars Technica 4 August 2011, http://arstechnica.com/security/2011/08/serious-security-holes-found-in-siemens-control-systems-targeted-by-stuxnet/

A CIVIL SOCIETY APPROACH

What should a cyber security agenda and strategy for civil society look like?

Civil society is not a homogeneous entity; it is composed of a variety of cultures, addresses a wide variety of issues, and includes a vast array of diverging opinions as to how different issues should be addressed. In some areas there is a convergence of interests amongst global civil society, in other areas there is a divergence of interests. However, civil society faces common cyber security challenges.

While generally civil society should be interested in an open internet that promotes freedom of expression and access to information, secure communications are also in its interest. Confidence in the security and privacy of communications infrastructures enables civil society to conduct its affairs without worrying about theft of money or information, or worrying about electronic surveillance.

Sometimes, measures to attain security, openness and privacy can work against each other. It is essential that cyber security initiatives protect the ability to use the internet to exercise the rights to freedom of expression and freedom of association. The means of securing networks should also not expose individuals to undue and illegal surveillance and must respect the right to privacy. Civil society needs to approach cyber security in a way that balances the concerns of these different rights.

A human rights approach to cyber security should put the security not just of states and government networks on the agenda, but also the security of business networks, civil society networks and organisations' networks. The security of individual users (netizens) also needs to be a central focus of a cyber security strategy.

Civil society needs to carefully decide whether to bring issues onto a national cyber security agenda, and whether or not these issues are dealt with better when they are on the national agenda of states. Civil society needs to consider the costs and benefits of securitising certain issues. Do the issues warrant the importance of national security status? Are they best dealt with through a national security or information security framework? Are they currently addressed by other government structures? Are there non-internet focused mechanisms or initiatives that are already dealing with these issues? Civil society needs to think carefully about when to securitise issues, and when not to securitise them. Will the securitisation of issues enhance or marginalise civil society's current role? Some issues may need to be securitised, some issues may need to be discussed and brought onto the cyber security agenda but not securitised, and some issues may need to be de-securitised.

Multi-stakeholder discussion must be fostered in debate about national cyber security strategies. Civil society needs to actively engage and demand multi-stakeholder participation in the formulation of national, regional and international cyber security policies and agreements. Civil society, the academic and technical community, internet users and content creators (netizens), the private sector, business, the military and intelligence agencies must all be present at the discussion. Multi-stakeholder cyber security discussions must be encouraged in existing multi-stakeholder forums like the IGF.

Cyber security governance needs to be addressed in a manner in which it does not supersede other internet governance issues. Existing policy making mechanisms on internet governance at the national to international level, should not be replaced by new exclusively cyber security focused policy-making mechanisms.

Cyber security policy must enhance the security of women human rights defenders (WHRDs), and make sure that national security strategies address violence against women, both online and offline.[45] WHRDs also need to build capacity around the use of important technological tools available to protect their operational and physical security – such as encryption or anonymity tools.

Finally, civil society must demand evidence-based discussions on cyber security. Due to the problem of attribution in cyber security, it is easy to make policy decisions on incorrect facts. Demands formulated by policy makers claiming cyber security incidents and threats must be backed by evidence.

[45] See also Danna Ingleton, "Let's stop our fear of tech leading to misuse of security legislation" GenderIT, 25 October 2012, http://www.genderit.org.

ASSOCIATION
FOR PROGRESSIVE
COMMUNICATIONS

A CYBER SECURITY AGENDA FOR CIVIL SOCIETY
WHAT IS AT STAKE?

APC is an international network of civil society organisations founded in1990 dedicated to empowering and supporting people working for peace, human rights, development and protection of the environment, through the strategic use of information and communication technology (ICTs).

We work to build a world in which all people have easy, equal and affordable access to the creative potential of ICTs to improve their lives and create more democratic and egalitarian societies.

www.apc.org info@apc.org

Graphic Design: MONOCROMO

Commissioned by the Association for Progressive Communications (APC).

Conducted with support from the Swedish International Development Cooperation Agency (Sida).

CONNECT YOUR RIGHTS!

A CYBER SECURITY AGENDA
FOR CIVIL SOCIETY. WHAT IS AT STAKE?
April 2013

APC-201304-CIPP-R-EN-P-186

ISBN: 978-92-95096-95-0

ISBN 978-92-95096-95-0

9 789295 096950