University of New South Wales
University of New South Wales Faculty of Law Research Series
2008

Year 2008 *Paper* 60

Anti-Censorship, Benevolent Payloads and Human Rights

Alana Maurushat*

*University of New South Wales

Anti-Censorship, Benevolent Payloads and Human Rights

The original publication entitled, "The benevolent health worm: comparing Western human rights-based ethics and Confucian duty-based moral philosophy" is available at www.springerlink.com

Alana Maurushat

Abstract

Computers and robots have long been used in "physical" environments where it is too dangerous, hostile, or difficult for humans to perform tasks. What about situations where the danger stems from political and legal environments? This paper will look at the ethical and legal use of a computer worm to perform anti-censorship tasks. Two specific scenarios will be examined. The first will look at the use of a computer worm to monitor and test Internet censorship of "the Great Firewall of China". The second will highlight the use of a worm for anonymous networks, and to deflect encryption detection through chaffing and winnowing. The third will look at the use of a computer worm to disseminate vital information in situations where public health is threatened by government censorship drawing on the health epidemics of AIDS, SARS and Avian Bird Flu in the People's Republic of China. Ethical and legal issues will be examined in a general fashion and then within the framework of human rights and Confucius moral philosophy. Technical and political issues will also be examined to the extent that they better inform the ethical debate.

Keywords

Human rights, computer worms, virus, hacker, malware, Internet, censorship, illegal technology, moral philosophy, human rights, public health, freedom of expression, privacy, anonymity, and access to information.

INTRODUCTION

Computers and robots have long been used in "physical" environments where it is too dangerous, hostile, or difficult for humans to perform tasks. What about situations where the danger stems from perils in political and legal environments? This paper will look at the ethical and legal use of a benevolent payload in a computer worm to perform anti-censorship tasks. Related anti-censorship tasks to be examined include firewall testing, chaff and winnowing, anonymity and information delivery. The first task will look at the use of a computer worm to monitor and test Internet censorship of "the Great Firewall of China". The second will look at the possible use of a worm to establish temporary anonymity networks. The last scenario will look at the use of a computer worm to disseminate vital information in situations where public health is threatened by

government censorship drawing on the health epidemics of AIDS, SARS and Avian Bird Flu in the People's Republic of China. The author uses China by way of example due to the extremity of the example, as well as her experience and familiarity with politics, censorship strategy and legal developments in the region.[1] Ethical and legal issues will be examined in a general fashion and then within the framework of human rights. Technical and political issues will also be examined to the extent that they better inform the debate.

The use of a controversial technology such as a computer worm to perform anti-censorship tasks in China presents contentious ethical and legal issues worth examining. When is the use of an illegal technology ethical? Does the dual use of a computer worm for malicious or benevolent reasons play a part in the analysis? If so, at what point? Is motivation the determining factor? Intended use? Actual consequences? Is there a moral duty to write and disseminate public health information which differs from authorized accounts? Is the duty a general duty or is it specific to certain members of society? Does the mode of information delivery play a part in the analysis? Are anonymous modes of dissemination less ethical than methods which provide accountability? To what extent does the source of the information factor into the equation? What role does risk of criminal sanction play in ethics? Does the risk of criminal sanction depend on the actual use or potential consequences of the technology? Does the violation of human rights justify the illegal activity? If so, is the Chinese context justifiable? Is the use of a benevolent worm compatible with Western ethical traditions? Chinese ethical traditions?

For the purpose of this paper, a brief definition of a benevolent worm will be provided with an overview of anti-censorship tasks including firewall testing, anonymity networks, and information delivery. An overall account will be given of the censorship environment in China. The censorship environment will be broken down into a general context, the "Great Firewall of China", and using the example of public health information. This will be followed by an account of technical aspects of the benevolent worm inasmuch as it will inform and frame the debate on ethical and legal issues. The core of the paper will examine ethical issues in a general fashion, and then in a specific manner drawing on the moral philosophy of civil liberties / human rights and through the lens of Confucius moral philosophy. The author will suggest how human rights and Confucius moral philosophy may be used to better understand and, to a certain extent, justify the use of the benevolent payloads in a computer worm. The application of the analysis could extend to an examination of the ethical use of illegal technologies.

WHAT IS A BENEVOLENT WORM?

A benevolent computer worm is a form of malware. Malware is the name for software with a malicious focus. Typically includes the following types of computers programs: virus, worm, Trojan horse, spyware, adware, spam, bot/agent, zombie, exploit, bug,

[1] For example, the author provided advice and coordinated a portion of the anonymous testing for the OpenNet Initiative study. OpenNet Initiative (2005) Internet filtering in China in 2004–2005: A country study. Available at http://www.opennet.net/china.

keylogging and so forth. The idea of a benevolent virus or worm is not novel. Early research and debate focused on the use of a worm to patch existing security flaws in software.[2] The idea of "good" viruses and worms that have a beneficial effect has been around since the earliest academic virus and worm research. For example:

- A virus could be written that compresses executable files to save disk space.[3] Infected/compressed files would be automatically decompressed by the virus as needed. This idea was realized by the Cruncher virus in 1993.[4]

- The KOH virus encrypts floppy disks and hard disk partitions for security reasons.[5] A legitimate user would know the decryption key and could access the files, i.e., KOH was not "ransomware" being used for extortion.

- Early worm research implemented a distributed computing framework at Xerox PARC.[6] After solving some problems controlling the worms, a variety of applications were built including network diagnostics and computing frames of a computer animation.

- A virus could perform system maintenance, like upgrading outdated versions of programs.[7]

- Predator worms are revisited periodically, the somewhat romantic notion that good worms can hunt down and destroy bad worms, or that good worms can find and patch vulnerable machines.[8] Real attempts at predator worms, such as the Welchia worm which tried to clean up after Blaster,[9] have generally proven disastrous and have resulted in more trouble than the original worm caused.

Each of the above examples relates to electronic commerce applications and typically involves the use of a viral propagation method to fix security flaws in a system. However, for each of these examples, the same tasks could be performed in another manner without the risk of using hard-to-control virus/worm propagation mechanisms. Typically security flaws are mended through 'patching'. A 'patch' is a piece of software

---

[2] Aycock, J. and Maurushat, A. (2006) 'Good' Worms and Human Rights. Technical Report 2006-846-39, Department of Computer Science, University of Calgary.
[3] Cohen, F. (1987) Computer viruses: Theory and experiments. Computers & Security, 6(1).
[4] Kaspersky, E. (1993) Cruncher – the first beneficial virus? Virus Bulletin.
[5] Ludwig, M. (1998) The Giant Black Book of Computer Viruses. American Eagle, 2nd edition.
[6] Shoch, J.F. and Hupp, J.A. (1982) The 'worm' programs – early experience with a distributed computation. Comun. ACM, 25(3).
[7] Cohen, F. B. (1994) A Short Course of Computer Viruses. Wiley, 2nd edition.
[8] Aitel, D. (2006) Nematodes – beneficial worms available at http://www.immunityinc.com/downloads/nematodes.pdf. Gupta, A. and DuVarney, D.C. (2004) Using predators to combat worms and viruses: A simulation-based study. 20th Annual Computer Security Applications Conference. *See also*, Hoyoizumi, H. and Kara, A. (2002) Predators: Good will mobile codes combat against computer viruses. Proceedings of the 2002 Workshop of New Security Paradigms.
[9] Perriot, F. and Knowles, D. (2004) W32.Welchia.Wrom. Symantec Security Response.

designed to fix problems with a computer program. Large patches are often referred to as 'service packs' or 'software updates.'

While a robust examination of types of malware is not required to understand the benevolent worms, a basic understanding of the differences between a virus and worm is essential, as the underlying technology of a worm alleviates some of the ethical and legal issues for its intended benevolent use.

A **virus** is a "block of code that inserts copies of itself into other programs". Viruses generally require a positive act by the user to activate the virus. Such a positive act would include opening an email or attachment containing the virus. Viruses often delay or hinder the performance of functions on a computer, and may infect other software programs. They do not, however, propagate copies of themselves over networks. Again, a positive act is required for both infection and propagation.

A **worm** is a program that propagates copies of itself over networks. It does not infect other programs nor does it require a positive act by the user to activate the worm. In this sense, it is self-replicating.

Irrespective of the characterization nearly all computer viruses and worms infect either software or hard-drives without the authorization of the computer owner. Similarly, all computer viruses and worms utilize bandwidth imposing a strain on traffic and resource demands. All computer viruses and worms may inadvertently cause unexpected damage to a computer system and may contain bugs. A benevolent worm is no exception. There are ways to minimize damaging effects of the worm through technical design. Such elements include: 1) slow-spreading, 2) utilize geo-location technology to limit its propagation within a region (".cn" and its equivalent for the Internationalized Domain Name in Chinese characters), 3) installation of short and reasonably shut-down mechanisms to avoid perpetual replication, 4) use methods requiring low-demand bandwidth, and 5) undergo professional debugging standards.[10]

Drawing on optimal design tailored to a specific desired function, a benevolent worm could perform many different tasks. The following sections intersperses the political and legal landscape of China with specific anti-censorship tasks performed by a benevolent worm. They are firewall testing, anonymity, and information delivery.

Firewall Testing

Many jurisdictions have a heavy censorship strategy for Internet content (for example, Vietnam, Saudi Arabia, and China).[11] Often testing occurs to discover what types of websites are blocked, and what types of information are deemed dangerous or taboo. Current methods of testing often involve remote techniques located outside of the jurisdiction. In order to validate the results, the same tests are performed by human beings located in state. This may involve risk of fines and imprisonment for in-state testers. An alternative way to perform the task uses a benevolent worm.

[10] Aycock and Maurushat, note 2.
[11] OpenNet Initiative study, note 1.

Anonymity
An anonymity network is a means by which a user can hide what they are connecting to – an attempt at accessing forbidden content might be detected, but an anonymity network would make it prohibitively difficult to trace the request back to its source.

A practical problem arises if mere use of a well-known anonymity network is enough to raise suspicion. The Tor anonymity network,[12] for example, supplies a list of Tor servers' IP addresses and ports. A connection to any of these ports is a clear signal that a bid for anonymity is being made.

Previous work has stated that malicious software could be used to automatically establish an anonymity network[13]. Benevolent worms could build such an anonymity network to provide anonymity service temporarily until filtering was changed to detect it.

Information Delivery
Where censorship policies are in play, there is often a need to access information in a many that is reliable, and safe. Anonymity networks do not always work nor are they necessarily the best alternative for certain tasks. In the case, for example, of the dissemination of vital public health information in the event of an epidemic, a benevolent worm could be used. Indeed, access to information may involve more than simply freedom of expression in this context.

FREEDOM OF EXPRESSION, ACCESS TO INFORMATION AND CENSORSHIP IN CHINA

Governments in China have traditionally utilized censorship as a means for control. Using censorship as a control mechanism has historically been pitted against the Chinese promotion of intellectual growth.[14] The rise of the Chinese Communist Party (CCP) brought with it the continued ideal of control over the dissemination of works and ideas. China continues to censor books, newspapers, and basically, most forms of publications that threaten the governing regime or criticize China's attitude towards human rights. [15] Included in this overall censorship strategy is tight control of the media and the Internet.

Media Censorship
All news agencies, including news websites and chatrooms, must be accredited. The redistribution and sale of foreign news in China may only be purchased and published from the state-run government news agency, Xinhua. Review and enforcement of laws and regulations is performed by two agencies (one for press, radio, film and television, and the other for written publications including the Internet), both of which are run by the

[12] Tor (2006) Tor directory protocol, version 2 available at http://tor.eff.org/svn.trunk/doc/dir-spec.txt
[13] Hirt, A. and Aycock, J. (2005) Anonymous and malicious. 15th Virus Bulletin International Conference.

[14] Reed, K. (2000) From the Great Firewall of China to the Berlin Firewall: The Cost of Content Regulation on Internet Commerce, 13 Transnat'l Law, 458.
[15] Reed, note 14, 459.

Communist Party's Central Propaganda Department (CPD). Against the backdrop of what could best be described as a labyrinth of laws and regulations, the CPD issues weekly informal directives to news agencies and Internet Service Providers (eg. Google and Microsoft) on news items requiring restrictive coverage.

Virtually all statutes and regulations concerned with communications (news or otherwise) contain vague language allowing authorities sufficient flexibility in determining which publications are in breach of the law.[16] Navigating through the ever-changing and complex media and Internet regulations is a seemingly never-ending process. While the regulations are ever-changing, there is a standard set of vaguely written provisions which appear in all such regulations: divulging state secrets; harming the honour or interests of the nation; spreading rumours which may disturb social order; and inciting illegal assemblies which could disturb social order – all punishable as a criminal offence. State secrets provisions are the most problematic as their wording and interpretation in practice has proven malleable to political will. It is difficult for writers (whether they be journalists or mere bloggers) to determine in advance whether their message would contravene the law.

Where writers publish illegal content they are subject to a number of punishments such as dismissal from employment, demotion, libel, fines, closure of business, and imprisonment. Imprisonment for illegal new stories extends to employees of foreign news agencies. For example, Hong Kong based journalist Ching Cheong (Singapore's Straits Times) and Zhoa Yan (New York Times) were arrested and detained for reporting articles about Communist Party leaders.[17]

Public Health News

Censorship in the area of public health has become increasingly important in many parts of the world for a number of reasons. Groups with a vested interest in a policy area are motivated to censor material. This may include governments, corporations, professions, and organizations. The censorship may be direct (legal sanctions) or indirect (corporate and individual self-censorship). As experts in the field, NGOs and other citizen movements champion competing visions of issues, the more incentive there may be to censor. This is true in a number of circumstances. For example, curtailing access to information regarding the health and welfare of soldiers in the Kuwait and Iraq wars, poor health conditions in Aboriginal communities, downplaying epidemics to bolster economies, and so forth. While there are many examples along the spectrum of public censorship, this paper's discussion of the benevolent worm will be limited to that public health information of the Peoples' Republic of China (China) drawing on three public health crises: HIV/AIDS, SARS and Avian Influenza.[18] In each of these situations, Chinese citizens faced a public health epidemic (which then spread to the international

[16] Zissis, C. (2006) Media Censorship in China. Council on Foreign Relations available at http://www.cfr.org/publication/11515/

[17] Reporters without Borders (2005) Government turns deaf ear to call for Ching Cheong's release, available at http://www.rsf.org/article.php3?id_article=13957

[18] Martin, B. (2001) Environment and Public Health, in Censorship: A World Encyclopedia, Vol. 2 (ed. Jones, D.). Fitzroy Dearborn, London.

community). In each of these situations the Chinese government heavily censored information, allowing the disease to unnecessarily spread faster in an uncontained manner. And in each of these situations individuals who vocalized or published unauthorized news articles on the epidemic (many prominent experts, doctors and activists) were detained without reason serving time in prison. Some were threatened or charged with divulging a state secret.

News around sensitive topics such as a public health crisis is heavily censored and monitored. Historically, individuals who reported and disseminated sanctioned public health news were often detained without reason and, in some cases, these individuals were charged with divulging a 'state secret'. Many academics and experts have written on the scope of 'state secret' in China. The notion of 'state secret' has traditionally been broad and deliberately ambiguous, while its scope of application is ever-changing.[19] It remains impossible to ascertain whether a person's actions would fall within a 'state secret'. People have been charged with this serious offence for the dissemination of banned information related to human rights, revealing draft laws (white papers), publishing unauthorised news reports, and publishing information critical of governing authorities. The act of circumventing the "Great Firewall" for illicit purpose, and mere research on Internet censorship, could conceivably fall within the parameters of 'state secret'. The CCP's unpredictable use of broad, ambiguous laws to deter freedom of expression is heavily criticized in the international arena. While 'state secret' laws remain a potent threat, the CCP has a number of criminal provisions which it regularly uses to curtail the dissemination of sanctioned information. To paraphrase a prominent Malaysian journalist Steve Gan, "We have the right of freedom of expression. The problem is that we have no rights once such words are freely expressed."[20] The same could be said of China.

Access to information may involve more than freedom of expression; timely information may have repercussions for the health and welfare of individuals. Indeed, there are three specific areas where censorship and a lack of accurate information distributed in a timely manner have had unrefuted consequences in China in recent history: AIDS, SARS and Avian Bird Flu.

HIV/AIDS: The Chinese government has suppressed and continues to suppress information on the spread of HIV / AIDS.[21] By 1987 the government had reported only 4 known cases claiming that AIDS was a foreigners' disease.[22] The lack of reporting and ineffective preventative measures led a number of people to become AIDS activists. These activists reported significant rates of people infected HIV and campaigned for the

---

[19] Hualing, F. (2005) Counter-revolutionaries, subversives, and terrorists: China's evolving national security law, in National Security and Fundamental Freedoms: Hong Kong's Article 23 Under Scrutiny. Hong Kong University Press.

[20] Steve Gan co-founded of on-line news distributor Malyskini.com. Words spoken at a conference organized by the Friedrich Naumann Stifung Instititute, New Communication Technologies in Asia: Surveillance, Cyber Security and Privacy; and Asian Politics and New Technology: Poor Bedmates? (November 2002).

[21] Settle, E. (2003) AIDS in China: An annotated chronology. Available at http://www.casy.org/chron/AIDSchron_11603.pdf.

[22] China Aids Survey available http://www.casy.org/chronpage.htm

government to take proactive measures to reduce the spread of this debilitating disease. Many AIDS activists, including the famous activist Wan Yanhai, have been detained and charged with divulging a state secret.[23] Infected blood supplies appear to have initially been the main source of the problem. Infected blood supplies, however, still taint China with many people in poorer areas donating blood for money while drug use, prostitution and a lack of educative measures continue to exacerbate the situation. The reality today is that China has one of the highest HIV / AIDS rates in the world outside of Africa. While we will never know the effect that accurate and timely information would have had in this epidemic, it is certainly plausible that access to such important information could have reduced the rate of infection.

SARS: Similar to the HIV/AIDS crisis, the Chinese government withheld critical health information on Severe Acute Respiratory Syndrome in 2002. China has a longstanding tradition of curtailing news deemed harmful to society and to China's image. In the case of SARS, it was thought that exercising tight media control would reduce public fear and lessen economic damage in the region.[24] The lack of reliable dissemination of information and the underreporting of infected SARS patients to the World Health Organization allowed the disease to spread more readily from Guangdong province to other provinces in China, to Hong Kong and to other countries in the world.[25] The SARS health crisis can be partially attributable to nondisclosure of pertinent information.

Avian Influenza (also referred to as bird flu): While avian influenze has not yet reached the level of crises of HIV/AIDS or SARS in China, historical events give clear signs that any information provided by Chinese officials should be perceived with caution.[26] It is believed that Quiao Songju, a Chinese farmer, was arrested and detained for reporting a potentially infectious bird in the Anhui province.[27] Prominent Hong Kong virologist, Guan Yi, was invited by the Chinese government to study ABF. His account of the disease was vastly different from the official version reported by the Chinese Government. Guan's publications are censored in China while it has been made known to the prominent virologist that he should not return to China. It is rumoured that Guan has been threatened with detainment and there is further speculation that he may be in violation of having disclosed a 'state secret'.

China's newly drafted censorship rules compound the situation. The newly drafted law states that it is a criminal act to publish any information on 'sudden events' without prior

---

[23] Chen, A. (2003) The limits of official tolerance: the case of Aizhixing, in AIDS and Article 23 (ed. Human Rights Watch China), China Rights Forum, No. 3, 51.
[24] Kalathil, S. (2003) Battling SARS: China's silence costs lives. International Herald Tribune.
[25] World Health Organization (2004). Severe Acute Respiratory Syndrome. Available at http://www.who.int/csr/don/archive/disease/severe_acute_respiratory_syndrome/en.
[26] *See* Washington United Press International (2005) Is China Hiding Avian Influenza? Available at http://www.terradaily.com/reports/Is_China_Hiding_Avian_Influenza.html . *See also* World Health Organization (2006). WHO urges Member States to be prepared for a pandemic. Available at http://www.wpro.who.int/media_centre/press_releases/pr_20060919.htm.
[27] United Press International (2005) Is China Hiding Avian Influenza? Available at http://www.terradaily.com/reports/Is_China_Hiding_Avian_Influenza.html

authorization from the Chinese Government. 'Sudden events' are defined as 'industrial accidents, natural disasters, health and public security issues'.[28] The government claims that the law is aimed at irresponsible journalists who report untruths potentially causing panic among the public. Critics have claimed that the draft law is aimed at preventing future disclosures of embarrassing news.[29] Public health epidemics would fall under the category of sudden events.

The Internet and the "Great Firewall of China"

The Internet and wireless technologies have been heralded as vehicles of free expression. It has generally been thought that no government could control information on the Internet, hence the expression "the Internet routes around censorship." In China, this is increasingly no longer true. The Chinese Government erected, through its Golden Shield Project, what has become known as the 'Great Firewall of China'.[30]

Access, control and censorship of Internet content in China is most often attributed to the 'Great Firewall of China'. This is, however, something of a misnomer; the firewall is merely one path in a maze of controlling technologies and non-technological means in an overall Internet censorship strategy. This censorship strategy is comprehensive, incorporating sophisticated technologies, numerous regulatory measures, market influences, and aggressive policing and surveillance of Internet activity, resulting in an atmosphere of self-censorship.

Laws regulating free speech and the Internet are implemented out of concern for the potential harm posed by unfettered access to sites that contain political, ideological, social, or moral content that the CCP perceives as harmful. China has adopted a comprehensive Internet censorship strategy utilizing a range of control mechanisms. Mechanisms of control include laws and regulations pertaining to physical restrictions, regulations of use, ownership and operation of Internet Service Providers (ISPs), Internet Access Providers (IAPs), and Internet Content Providers (ICPs).[31] Similar to media regulations, a series of ever-changing Internet regulations are also relevant to the dissemination of information. Authorized access entails individuals having to obtain licenses for Internet access. In order to obtain a license, individuals are required to register with the local police and provide their names, the names of their service provider, their e-mail addresses, and list any newsgroups in which they participate. This, of course, does not mean that anonymity and pseudonymity cannot be achieved for Chinese cybersurfers. Users have flocked to cybercafés and universities to access the web. The CCP has responded by shutting down many cybercafés, then later by requiring all cybercafés and universities to obtain user identification, and to keep detailed logs of user activities (the regulations are complex and comprehensive). The extent to which such

[28] Qinglian H. (2006) New Regulations in China Target Foreign Media, The Epoch Times available at http://www.en.epochtimes.com/news/6-9-28/46453.html

[29] Ching, F. (2006) China's media censorship, Korea Times available at http://www.asiamedia.ucla.edu/article.asp?parentid=48789

[30] Chase, M. (2002) You've Got Dissent!: Chinese Dissident Use of the Internet and Beijing's Counter-Strategies. RAND, National Security Research Division Center for Asia Pacific Policy.

[31] Liang, C. (2001) Red Light, Green Light: Has China Achieved Its Goals Through the 2000 Internet Regulations, 34 Vand. J. Transnat'l L. 1417, 1428.

entities have fully complied with the law in practice has not been explored, but the threat of surveillance continues to lead to an environment of self-censorship. The ability to access banned documents and to communicate anonymously is challenged.

Information flows from the Internet subscriber (home, cybercafé) to the Internet Service Providers (ISPs) to four gateways controlled by the Ministry of Posts and Telecommunications[32]. ISPs are regulated through a myriad of laws which are, again, ambiguous and complex. It is difficult for any party to know if they are in compliance with the law. The regulations require ISPs to restrict and control access to harmful/banned websites, allow surveillance software on their systems, and keep logs of user activity.[33] Email is neither private nor anonymous when using an ISP regardless of whether a domestic or foreign service is used. ISPs must and do comply with requests to reveal personal information of the true identity of users as well as information about email content. For example, both Yahoo!China and Yahoo!HK, on informal request from Chinese authorities, have disclosed the address and computer port number of several journalists.

Recent popular methods for dissemination of taboo/illegal documents include spam, weblogs and chatrooms – all delivery methods involving the Internet which allow for some degree of anonymity or pseudonymity. Chinese officials have recently begun to crack down on weblog and chatroom use, introducing a host of new regulations directly targeted at information deemed harmful to Chinese society. China's filtering/anti-spam technology has likewise greatly evolved so that spam has become a less effective means of communicating information. Those who continue to engage in the exchange of banned communications, whether it be via spam, weblogs, text message or other fora, potentially face criminal charges. As the regulations are written in the traditional fashion of ambiguously overbroad provisions, the reality is that merely opening a spam message known to contain harmful material, or forwarding the message *could* be a contravention of the law.

Is it possible to route around censorship in China? Circumventing the 'Great Chinese Firewall' is achievable using a number of different methods which range from the use of web proxies (Tor, Anonymizer, Dynapass, Psiphon) to accessing the Internet in peak times (State surveillance requires a large amount of bandwidth), to the use of encryption services. Proxies such as Tor may still be blocked at the node level (although currently they are not). It would be possible to use a benevolent worm to quickly install a temporary anonymity network. While State surveillance requires large amounts of bandwidth, the threat of legal and economic sanction plus self-censorship – ISPs restricting access to potentially contentious sites, cybercafés and universities discouraging banned websurfing, individuals refraining from accessing even potentially illegal material – effectively fills the gap left by technological constraints.

---

[32] The precise number of gateways has not been established. Some report 3, other 4, and others 5. The author has taken the middle figure as an average only. This ambiguity illustrates the cloud that shrouds accurate information pertaining to the 'Great Firewall'.

[33] Liang, note 31.

The use of encryption is able to circumvent filtering and keyword sniffing technology at the router level, but this does not provide a safety net for those wishing to disseminate contraband information. As stated previously, ISPs must and do comply with requests to disclose personal information. Many ISPs have also built censorship functions into their encryption technology. Activists using the encrypted Skype technology, for example, have been cautioned against its use due to built-in censorship functions.[34] Encrypted messages may arouse further suspicion which may lead from monitoring of general data traffic over the Internet to the surveillance of specific individuals and groups. Regardless of the method employed, the threat of criminal sanction is always a possibility.

The ability to use the Internet to publish sanctioned information is a risky proposition. Assuming that there are strong ethical arguments in favour of disseminating sanctioned information a new mechanism will be required for large-scale information delivery. A worm with a benevolent payload provides one possible solution.

In the case of the Great Firewall, even the extent of the censorship is not apparent. Attempts to access forbidden material yield results akin to network or server problems.[35] Accurate glimpses into the censorship mechanism are rare, like the discovery of a list of banned words shipped with Chinese instant messaging software.[36] Moreover, the consensus is that Chinese censorship is a dynamic work in progress, and subject to frequent changes.[37] Groups with interests in human rights, freedom of expression, and privacy monitor the extent of Internet censorship in China and elsewhere. For China, the current methods of testing are listed below. All the tests originate outside China unless otherwise noted.

- Fetch URLs containing forbidden terms from Chinese web servers.[38] This testing is based on the supposition that the Firewall's operation is symmetric, and censors the same material coming and going. It is not a complete test because coarse-grained censorship like blocking of IP addresses is not examined.

- Fetch URLs whose web pages possibly contain sensitive content, via dialup modem to Chinese ISPs. This method was eventually made unusable.[39]

- Fetch URLs whose web pages possibly contain sensitive content, through Chinese open proxy servers.[40]

---

[34] Human Rights Watch (2006) How Censorship Works in China: A Brief Overview, available at http://www.hrw.org/reports/2006/china0806/3.htm
[35] Zittrain, J. and Edelman, B. (2003) Internet filtering in China. IEEE Internet Computing. See also, OpenNet Initiative, note 1.
[36] Qiang, X. (August 30, 2004) The words you never see in Chinese cyberspace. China Digital Times.
[37] OpenNet Initiative, note 1.
[38] Clayton, R. Murdoch, S.J> and Watson, R.N.M. (2006) Ignoring the great firewall of China. 6th Workshop on Privacy Enhancing Technologies.
[39] Zittrain, J. and Edelman, note 35.
[40] OpenNet Initiative, note 1.

• Examine the results from Chinese search engines, when searching for particular web sites and keywords.[41] Here, the testing was done from both the U.S. with a U.S. ISP, and from China using a Chinese ISP.

• From within China, fetch URLs entered manually or fetch URLs *en masse* using a program. The URLs were entered, and the program was run, by volunteers.[42]

Where applicable, controls are used to distinguish censorship from legitimate network and server failures. These tests are not without their share of problems. They can suffer from 'limited scope'. Differences have been observed between proxy server tests and in-state tests; given that over 70% of Chinese in a survey claim not to use proxy servers anyway[43], in-state tests are really the best way to get an accurate idea of what the typical user sees (and doesn't see). However, in-state testing entails risk for the humans who perform it.

ETHICAL BENEVOLENT PAYLOADS?

Malware refers to computer software which either acts maliciously or whose effects are malicious – the two are not necessarily synonymous. In a wider context, malicious would extend to any type of computer code installed without consent regardless if any damage occurs to the computer. This appears to be the opinion of leading world IT expert Bruce Schneier describes the use of a benevolent payload to perform patching functions as:

> "Patching other people's machines without annoying them is good; patching other people's machines without their consent is not … Viral propagation mechanisms are inherently bad, and giving them beneficial payloads doesn't make things better."[44]

Under this definition, no malware could be construed as benevolent. The weakness of this argument is that its discussion has been limited to patching and similar e-commerce activities, where consent is desirable from a corporate ethics perspective and is necessary in order to conclude a binding legal contract. Missing from this discussion is the application of a benevolent worm outside of the e-commerce realm, along with the discussion of the difference between consent and informed consent, the latter being the legal requirement in most jurisdictions.

The subject of informed consent in the digital age is contentious. It has been argued that consent is given in most Internet applications through checking the "I Agree" button of end-user license agreements and privacy policy statements. This is not necessarily

[41] Human Rights Watch (2006) Race to the bottom: Corporate complicity in Chinese Internet censorship.
[42] OpenNet Initiative, note 1.
[43] Liang, G. (2005) The CASS Internet report 2005: Surveying Internet usage and impact in five Chinese cities.
[44] Schneier, B (2003) Benevolent Worms, Crypto-Gram Newsletter, available at http://www.schneier.com/crypto-gram-0309.html.

representative of informed consent. Most users do not read terms of use. When they do, such licenses contain onerous obligations unilaterally imposed on them expressed in complex, aggressive legal rhetoric – most of these types of terms remain untested in law and run against the basic tenants of the law of contracts, namely consideration, meeting of the minds, and adequate notice of change of terms. The United States represents a notable difference from other jurisdictions. The recent judgments of *Ticketmaster v RMG* and *Southwest v Boardfirst* have upheld vague terms in the more controversial type of end user license agreement known as a browsewrap.[45] It remains to be seen whether appellant level courts will follow the line of reasoning in these two lower court decisions, especially given the disputed terms of use were between commercial competitors. Consent in many terms of use is illusory at best. [46]

The intricacies of informed consent are perhaps best illustrated by way of example. Many corporations, such as Sony, release products with an end-user license term authorizing them to utilize rootkits, backdoors and digital rights management systems for a variety of unspecified purposes, all of which may be subject to change without notification to the user.[47] The rootkits, in turn, render computers vulnerable to intruders to install malicious applications onto their computers. Digital rights management systems allow monitoring devices which track the use of a work (for example, a music c.d.), which could theoretically be used as evidence to bring legal suits against those who make illegal use of the copyrighted work. The author uses the example of consent to illustrate the discrepancy between tangential concepts of theory and practice. The author agrees that informed consent is a desired feature in software distribution mechanisms. Concluding that consent is required in all contexts is to prematurely rule on an issue which has, so far, only been discussed in the limited context of electronic commerce.

If consent is gained, do benevolent payloads become ethical? If there is no consent, are benevolent worms precluded from becoming ethical? It appears as though the debate on consent and malware has inherited the intellectual baggage of assumptions surrounding consent. Nowhere is this better articulated than in the famous essay by Robin West, "Authority, Autonomy, and Choice: The Role of Consent in the Moral and Political Visions of Franz Kafka and Richard Posner."[48] West exposes the fallacy in Posner's theory that choice and consent in a legal system allow for an increase both in morality and autonomy. Within the confines of benevolent payloads, there is an assumption that lack of consent is inherently bad or unethical contrasted with acts where a vague notion of consent is obtained, thereby magically summoning the requisites of legal and ethical

---

[45] See the lower court decisions of *Ticketmaster L.L.C. v RMG Technologies*, 2007 WL 2988403 and *Southwest v Boardfirst*, No;3 06-CV-0891-B

[46] For an excellent article outlining specific assessments of terms of use see Lemley, M. (2006) Terms of Use, Minn L Rev.

[47] Several class actions suits were launched against Sony around the world. For example, see *In re SONY BMG CD Technologies Litigation* No 1:05-cv-09575 (NRB) Access at: <http://www.eff.org/IP/DRM/Sony-BMG/sony_settlement.pdf>

[48] West, R. (1985) Authority, Autonomy, and Choice: The Role of Consent in the Moral and Political Visions of Franz Kafka and Richard Posner. Harvard Law Review, Vol. 99, No.2.

action. The presence of consent should be regarded as one component in an analysis of all factors contributing to an ethical framework.

An effects analysis would look to whether any tangible damage, other than use of bandwidth, has been done to the computer, webserver or user, or in the event that other types of damage are sustained, whether there are compelling reasons to derogate from the principles of user consent and avoiding damaging third party property. More importantly, an effects analysis would address the issues of when it is permissible to utilise bandwidth and install software on a user's computer without their consent. When, if ever, does a benevolent payload become permissible or mandatory as a moral duty?

The benevolent worm would be an information delivery method with worm-like characteristics. A computer worm is a self-replicating computer program containing a tailor-designed payload. The payload would be programmed to spread from computer to computer in China with the specific function of displaying the information in a pop-up window, or override a user's default web page with one displaying information.

In the case of the benevolent worm, the message would contain vital information relating to a public health crisis otherwise unavailable through traditional media sources. The information would ideally come from a trusted source containing accurate and truthful information (see discussion in following sections). The payload would be carefully programmed to prevent any deliberate or positive technical action by the recipient. The recipient would, therefore, have no knowledge or control of the worm. The latter points require elaboration. The self-replication method of worms is ideal in this situation as it is only the infected computer which takes part in the dissemination of sanctioned information; the person whose computer is infected is technically prohibited from any deliberate or accidental positive acts, and has no control or knowledge of the worm. In order to achieve this, the pop-up message generated by the worm must have the following features:

- must not be a virus in that it must be self-replicating,
- not contain links to additional sources of information,
- the user would not be able to save the information to his or her computer,
- the user could not forward the message to others, and
- the information would disappear from the system altogether after a specified amount of time.

In the case of the latter, the pop-up would appear for a specified time (eg. 10 minutes) and re-appear each time a person turned on their computer for a programmed length of time (eg. 2 weeks). At the end of a short period of time (eg. 2 weeks) the worm would completely disappear from the user's computer system – all technically feasible through the programming of the payload. These features greatly reduce if not eliminate any risk to the recipients of the information. All elements necessary to prove a criminal act are removed: positive act, knowledge or foreseeable knowledge, mens rea, and motive.

A chief criticism of the use of viruses and worm for benevolent purposes is that there are safer alternative means of achieving the same goal.[49] The same cannot be true with the benevolent worm. Alternative means of health distribution would include: illegal news reporting; illegal dissemination of news domestically through a blog, chatroom or spam; spam techniques from a foreign jurisdiction; and access to materials outside of China through anonymizing technologies such as web proxies. A common flaw of these methods is the necessity of a *positive act by both the sender and recipient* of information, this is especially so for the first two means. A positive act, whether it is through technical (eg. virus) or manual (eg. forward spam message) would allow for the possibility of dual criminal charges. Meanwhile there are further challenges with the latter two distribution means of foreign spam and web proxies. As pre-eminent human rights activist Sharon Om has noted, human rights spamming lists are potentially illegal under the United States Can Spam Act.[50] The use of anonymizing technologies such as web proxies is by no means fool proof. Such technologies are capable of being blocked (policy choice not a technical feat), even trust-enabled web proxies such as psiphon. [51]

In the case of the benevolent worm, only the sender of the information would perform a positive act. These acts would still be illicit on many fronts but only the sender would bear risk.

The programmer of the human rights worm will be in violation of computer misuse law. In the event that the computer programmer is not necessarily the person or group who distributes the worm; those individuals responsible for "letting the worm loose" could face criminal and civil charges. Finally, the authors of the actual information appearing in the pop-up screen may be charged with a number of criminal acts including state secret and possibly the new law on disclosure of non-authorized news on 'sudden events.' Positive acts are performed by those actors along the sender chain while recipients of information remain removed from the process short of reading the content in displayed in the window. Stated another way, the benevolent worm potentially offers a way to restore an individual's right to physical and mental well-being through a method that reduces the risk of persecution for those who disseminate un-authorized information and removes (potentially altogether) the risk for those who receive the information.

The above scenarios, however, envision the propagation of the worm and information writing to be performed by individuals within China. Such risks could be greatly reduced by creating the worm outside of China. While it is true that computer misuse is illegal in most jurisdictions, the threat of sanction depends greatly on political will. With open American support of projects which address human rights and democracy in suppressed regions, Congressional hearings on Internet censorship in China and, more specifically, US corporate compliance and aid in censorship; and the passing of the Global Internet Freedom Act, it is hard to believe that, at least in the United States, that there would be

[49] Bontchev, V. (1994) Are "Good" Computer Viruses Still a Bad Idea? In Proceedings of the EICAR '94 Conference.
[50] Hom, S., Tai, A., and Nichols, G. (2005) Human rights and spam: A China case study. Spam 2005: Technology, Law and Policy, 63.
[51] Psiphon available at http://www.psiphon.civisec.org/faq1.html

political will to prevent the benevolent worm. If anything, there may be available funding.

There is a strong psychological and political element to the creator (and disseminator) of the worm. A worm created inside China would have the distinct advantage of appearing to be change from within; a worm created outside China raises issues of external meddling, sovereignty, imperialism, or worse yet, information warfare. These issues will be more fully integrated into the ethical discussion below.

JUSTIFICATION OF BENEVOLENT WORMS

The ethical dimensions of a benevolent worm encompass several layers. A more sophisticated approach would be to treat the layers as information branches in the total infosphere.[52] For the purpose of this paper I will adopt a simpler approach referring to the author/producer, sender/distributor, recipient, content, delivery method and medium of communication.

One great concern in the propagation of a worm is that of trusted source. Trusted sources may be divided into two groups. The first involves the content of the information. The second relates to the information producers – authors and distributor. The 'who' in 'who says what' may be more important than the 'what'. The following analysis, therefore, assumes that it is possible to utilize trusted sources.

Human Rights

Western-based rights treatises, in particular human rights frameworks, may provide some justification of for a benevolent worm.[53] Human rights or civil liberties frameworks operate on two theoretical models. The first is one related to public international law where States bind themselves to legal obligations contained in treaties. The second involve the universality principle of human rights based on moral rights not legal rights.[54]

Under a legal rights based theory, specific rights and obligations are only provided to the extent of treaty provisions in international law. Such rights may or may not be entrenched in domestic / national law. Where rights are protected under international law, they may contradict and clash with domestic law. The nexus between national and international law has been discussed using the theories of dualism and monism. As the Honorable Justice Kirby writes:

> "For the monist, international law is simply part of the law of the land, together with the more familiar areas of national law. Dualists, on the other hand, assert that there are two essentially different legal systems.

---

[52] Floridi, L. Information ethics, its nature and scope, in Moral Philosophy and Information Technology (eds. J. van den Hoven and J. Weckert), Cambridge University Press, Cambridge.

[53] For an excellent treatise on human rights and civil liberties *see* Provost, R. (2002) International human rights and humanitarian law. Cambridge University Press. *See also*, Brems, E. (2001) Human Rights: Universality and Diversity. Kluwer International Law. *And* Blau, J. (2005) Human Rights: Beyond the liberal vision. Rowman and Littlefield Publishers, Lanham.

[54] Sandel, M. (1982) Liberalism and the limits of justice. Cambridge University Press.

> They exist "side by side within different spheres of action – the international plane and the domestic plane." [55]

The clash between national and international law is influenced by whether a court adopts a monist or dualist position. The Chinese government and courts use a dualist theory where human rights are viewed as a matter of 'foreign affairs.' As one human rights expert writes, "the Chinese government essentially views these obligations as a matter of foreign affairs, and seeks to insulate the domestic arena from the reach of international human rights law, both in symbolic and practical terms."[56]

International tribunals and courts also adopt a dualist approach. National law is treated as a fact. An obligation in international law cannot be avoided or excused due to a clash with domestic / national law.

Other governments and courts adopt a monist approach. This can be seen in the erosion of the dualist approach in many countries such as Australia and Canada. There have been many court decisions which integrate international law principles into the national landscape.

The second level relates to the universality of human rights. Universality is not a legal proposition but a moral one; that human rights are naturally acquired at birth regardless of the area of the world where you reside. Human rights subsist regardless of international and domestic legal obligations.

Regardless of the interpretation of human rights, benevolent anti-censorship worms represent undisputed legal and moral rights which may be stated in a simple form: everyone has the right of freedom of expression. In the case of a worm used to deliver public health information, the entrenched freedom extends to the enjoyment of the highest attainable standard of physical and mental health. These rights are legally protected in a number of international, regional, and United Nations Treaties to which China is party, and, according to the model of human rights one adheres to, are inherently entrenched regardless of the law.[57]

The Constitution for the People's Republic of China (PRC) recognizes "freedom of speech", however, the concept of free speech is viewed differently in China than in western democracies. Reed, an expert on freedom of expression in China, notes:

> "The PRC believes that rights are only instruments for realizing state

---

[55] Kirby, M. The Growing Rapprochment Between International Law and National Law, available at http://www.hcourt.gov.au/speeches/kirbyj/kirbyj_weeram.htm

[56] Woodman, S. (2005) Human Rights as "Foreign Affairs": China's Reporting Under Human Rights Treaties, 35 Hong Kong Law Journal 1.

[57] China is party to the following international treaties relating to freedom of expression and public health: the Universal Declaration of Human Rights (UDHR), International Covenant on Economic, Social and Cultural Rights (ICESCR), Convention on the Rights of the Child (CRC), International Covenant on Cultural and Political Rights, and Convention on the Elimination of All Forms of Discrimination against Women (CEDAW).

> objectives. Individual rights are merely residual freedoms found within the confines of the law. If necessary, all rights must be sacrificed for the good of the common collective. As a result, China traditionally keeps the dissemination of information and freedom of expression to a minimum. The CCP controls all facets of government, including the freedom of expression granted in the Constitution."[58]

Several distinct questions surface as a result of the above passage. Is China within its legitimate sovereign right to censor free speech on public health issues on the grounds that such discourse falls under the exemption of "national security"? Is civil disobedience justified in the context of disobeying the law for a higher purpose whether it be construed as a moral obligation or interpreted as for the greater good of the community (emphasis here on worm created within China)? Would a worm created outside of China be a deliberate act of interference with a nation's sovereignty? Under what circumstances might a benevolent worm be construed as part of information warfare?

Information dissemination as 'national security' threat

According to one view, national security always trumps individual rights because security, on a Hobbesian-type view, is necessary for a peaceful society in which persons can enjoy their liberty and rights. This view appears to be gaining adherents at least among legislators.

On the moderate viewpoint, free speech rights are defeasible, but only when appropriate justification for censorship is available. In order to protect free speech rights, legislative limitations on censorship powers are necessary. In a rights-respecting society, balancing involves prioritizing different rights in the case of *prima facie* conflicts of rights. In the case of liberal democracies, there should be strong limitations on violations of freedom of expression and liberty. On the other hand, as we have seen in the quotation from Reed, above, from the perspective of the PRC, rights are merely instrumental to the common good, and balancing rights can be done by determining what maximizes the common good. Rights can be overridden whenever the common good requires.[59]

Under public international law, governments are allowed to restrict the free flow of information to protect interests such as national security or public morals. National security ideology has, however, been used by authorities to justify human rights infringement. For this reason, international documents and principles were developed to keep rights exemptions confined to narrow determinations. For example, the *Johannesburg Principles on National Security, Freedom of Expression and Access to Information*[60] adopt a standard whereby freedom of expression and access to information

---

[58] Reed, note 14.

[59] Hagen, G. and Maurushat, A. (2005) Surveillance, Technology, and National Security: Issues in Civil Liberties, course materials , Asia-America Institute in Transnational Law

[60] Available at http://hei.unige.ch/humanrts/instree/johannesburg.html

may only be restricted where a number of conditions are met: prescribed by law, protects a legitimate national security interest, and is necessary in a democratic society. For example, a legitimate national security interest is incitement to violent overthrow of a government. National security restrictions are not justifiable in the case, for example, of "embarrassment or exposure of wrongdoing, or to conceal information about he functioning of its public institutions …" (principle 2(b)). China's restrictions on free speech and access to information clearly do not adhere to the Johannesburg Principles or other international standards for protecting the right to information. As Human Rights Watch notes,

> "Prior censorship in particular is severely disfavoured in international law, and not permitted in many constitutional systems. A decision to block access to online material should be subject to the highest level of scrutiny, with a burden on the government to demonstrate that censorship would effectively avert a threat of irreparable, imminent, and weighty harms, and that less extreme measures are unavailable as alternatives to protect the state interest at issue. At present, it seems apparent that China engages in no such scrutiny … "[61]

Moreover, the decision to punish certain speakers merely for exercising their right to speak frankly online (or off) is arbitrary and unpredictable with no opportunity for an individual or group to know in advance whether their actions comport with the law.

Conscientious Objection and Civil Disobedience

I will refer to two general types of civil disobedience. The first is better known as 'conscientious objection' where the moral agent performs or abstains from performing an act to preserve the agent's own moral integrity. In the case of a benevolent worm, a number of parties including the author/producer, and sender/distributor may feel morally compelled to receive or send what they believe is vital information otherwise not available within China. Conjecturing on the moral agent's dilemma, the agent is motivated to break the law in order to achieve a number of possible goals such as informing the populace of important news related to the epidemic and to encourage behaviour associated with containing the disease in question, or to access illegal materials related to the Falun Gong.[62]

The other type of disobedience, on the other hand, is known as 'civil disobedience' in the sense that it, "is conscientious disobedience of the law directed primarily … at bringing about a change in a law, policy, institution that is morally unjust or otherwise morally unacceptable … or a law which may be acceptable in itself but which is disobeyed in order to protest against the offending law."[63] The moral agent, in this instance, is

[61] Human Rights Watch, note 34.
[62] McCloskey, H.J. (1980) Conscientious Disobedience of the Law: Its Necessity, Justification, and Problems to Which it Gives Rise, 40, Philosophy and Phenomenological Research, 4.
[63] McCloskey, *ibid.*

motivated to affect change in the law. In the case of the benevolent worm, however, this would likely be a possible ancillary effect rather than a primary goal.

Conscientious objection and civil disobedience have been justified on a number of grounds.[64] One thought is that disobedience of the law may be justified where there is no disrespect or harm to others. Another ground speaks to a utilitarian approach of bringing about useful reconsideration of public policy, respect for human rights, interests of minorities and disadvantages groups, and actual reform of the law. It has been shown that other methods such as news reporting and spam potentially create harm not only for the sender but also for the recipient of sanctioned health information. Other firewall testing methods likewise impose risk of sanction. The benevolent worm has the goal of safely minimizing harm to the sender and attempts to eliminate harm to the recipient (realizing, of course, that unintended consequences are not always foreseeable). Many philosophers have specified that justifiable civil disobedience ought to be non-violent with the agent ready and willing to accept punishment as a consequence for breaking the law. This view seeks to disassociate civil disobedience from revolutionary disobedience. The author suggests that this dichotomy is more useful in a democratic state whose political leaders and citizens first have respect for their Constitutions and second for human rights in general. The dichotomy, therefore, seems less appropriate for autocratic states with documented histories of human rights abuse.

Sovereignty

Would a worm created outside of China be a deliberate act of interference with a nation's sovereignty? The answer to this question may lie in the meaning of sovereignty. In modern international law the notion of sovereignty is "people's sovereignty rather than the sovereign's sovereignty … [whereby] no serious scholar still supports the contention that internal human rights are "essentially within the domestic jurisdiction of any state" and hence insulated from international law."[65] The notion of sovereignty in human rights is, therefore, predominantly premised on democracy and rule of law. China is not a democratic nation adherent to the rule of law. It does not, however, follow that China is not entitled to sovereignty but rather, that issues of sovereignty are burdened with additional questions.

Yet sovereignty has generally been understood as one nation interfering with another nation's legitimate right to runs its affairs. One thinks of the invasion of Iraq and not generally of information on public health endemics. Sovereignty issues may be affected by the 'who' in 'who says what'. A worm released by the Canadian government, for example, could conceivably be construed as intentional sovereign interference. A worm released by an NGO, on the other hand, would be less likely to be perceived as sovereign interference; this would be further buttressed by a trusted NGO with strong links to China.

---

[64] Lyons, D. (1998) Moral Judgment, Historical Reality, and Civil Disobedience, 27, Philosophy and Public Affairs, 1.

[65] Reisman, M. (1990) Sovereignty and Human Rights in Contemporary International Law, 84, The American Journal of International Law, 4.

Information Warfare

In an extreme circumstance a benevolent worm might be construed as part of information warfare (IW). Defined simplistically, information warfare refers to, "actions taken to affect an adversary's information and information systems while defending one's own information and information systems."[66] There are six broad components to IW: physical attack / destruction, electronic warfare, computer network attack, military deception, psychological operations, and operations security. It is difficult to conceive how a benevolent worm in its described applications in this paper would fit into any one of these categories. One cannot, however, rule out the possibility of a worm with false and potentially harmful information to be released as part of an overall IW strategy. A strategy of disinformation, however, is applicable in a number of contexts including conventional means of information dissemination such as false news reporting, spam, and so forth. Careful attention to trusted sources could reduce the risk of the worm being perceived as IW.

Asian Values

At its most base conception, 'Asian Values' emphasize the community as opposed to the individual or self. It has been argued that human rights are incompatible with 'Asian Values'. Expressed more poignantly by Samuel Huntington:

> "the traditionally prevailing values in East Asia have differed fundamentally from those in the West and, by Western standards, they are not favourable to democratic development. Confucian culture and its variants emphasize the supremacy of the group over the individual, authority over liberty and responsibility over rights."[67]

Expressed somewhat differently, Western human rights-based rhetoric focus on rights of an individual whereas Eastern Confucius moral philosophy focuses on the duties of an individual to the community.[68] The following analysis places ethical debate on the benevolent worm in the Confucius moral philosophy tradition.

Confucius Moral Philosophy[69]

Confucius moral philosophy is often referred to as a duty-based philosophy. Confucian ethical teachings are grounded in five moral values: *Li* (ritual), *Hsia* (filial piety, duty to family), *Yi* (righteousness), *Xin* (honesty and trustworthiness), *Ren/Jen* (benevolence,

---

[66] Yoshihara, T. (2001) Chinese Information Warfare: A Phantom Menace or Emerging Threat? The Strategic Studies Institute, available at http://www.strategicstudiesinstitute.army.mil/pubs/2001/chininfo/chininfo.htm

[67] Hungtington, S. (1993) American Democracy in Relation to Asia: Democracy and Capitalism: Asian and American Perspectives (eds Bartley, R. et al.) Institute of Southeast Asian Studies, Singapore, p.28.

[68] Lee, S-H. (1996) Liberal Rights or/and Confucian Virtues? Philosophy East and West, 46, 3.

[69] *See* Fingarette, H. (1972) Confucius – the secular as sacred. Harper Torchbooks. See also Shun, K-L. and Wong, D. (2004) Confucian Ethics: A comparative study of Self, Autonomy and community. Cambridge University Press.

social virtue, humaneness towards others), and *Chung* (loyalty to the state). The Confucius view of duty was not traditionally extended to all people but was limited to five relationships: ruler to subject, father to son, eldest brother to younger siblings, husband to wife, and elders to juniors. There has never been a duty from human to human in traditional Confucius thought. Two contentious issues are raised in applying Confucius teachings to a benevolent worm. First, the values of *ren*, benevolence towards others, may compete with that of *chung*, loyalty to the state. Second, there is no general duty between humans outside of the five relationships.

The value of *chung* requires a person to be loyal to the state but not at any cost.[70] Confucius writes, "If a ruler's words be good, is it not also good that no one oppose them? But if they are not good, and no one opposes them, may there not be expected from this one sentence the ruin of his country?" [The Analects]. The most important value as espoused by Confucius was *ren*. A major component of ren involved individual self-cultivation in virtuous action. It has further been suggested that *li* – norms of social ritual and interaction – is a critical component in analysing *ren*. *Li* is learned by socializing and interacting with persons who embody ren.[71] As Lai writes:

> "The paradigmatic man is a creator of standards rather than a follower … and he possesses a keen sense of moral discrimination. Moral achievement reaches its culmination in those who have attained the capacity to assess events and who, being attuned to *li*, embody a sense of rightness."[72]

Good governance and social order were derived from a hierarchical chain of individual virtuous action thus it is written that, "their hearts being rectified, their persons were cultivated. Their persons being cultivated, their families were regulated. Their families being regulated, their States were rightly governed. Their States being rightly governed, the whole kingdom was made tranquil and happy" [Great Learning][73]. What of the case where *ren* is not personally cultivated leading to poor governance? Loyalty to the State is loyalty to a righteous government who has fulfilled its duties to its citizens in the spirit of *ren*; loyalty to the State has never been an absolute.

By no means does the author suggest that the overall governance of China has been poor under the current administration. China has had to face many problems that other nations, and in particular wealthy democratic nations, have never had to address: starvation, extreme poverty, territory occupation, a devastated economy, and population explosion to name but a few. While China has overcome many hurdles to better provide

---

[70] Beaudoin, C., Mizuno, T. and Winfield, B. (2000) Confucianism, collectivism and constitutions: Press systems in China and Japan. Communication Law and Policy, 5,3.
[71] Lai, K. (2006) Learning from Chinese Philosophies: Ethics of Interdependent and Contextualised Self, Ashgate World Philosophies, p.61.
[72] Lai, *ibid*.
[73] *The Great Learning, in The Chinese classics Vol. 1(translated by Legge), SMC Publishing, Taipei (1991).*
See also, Confucius (1991)Confucian Analects, in The Chinese classics Vol. 1 (translated by Legge), SMC Publishing Taipei.

for its people, its record on factors contributing to human dignity is poor (freedom of expression, protection of minorities, access to important and timely information, and so forth). It is within this limited latter context of human dignity that it is conceivable to characterize governance as poor. For instance, the manner in which public epidemics such as HIV/AIDs, SARs and Bird Flu has been handled is evidence that the government has not fulfilled its duties to the extent required under the spirit of *ren*.

The formation of a person's character through virtuous action is strongly tied to a sense of community and to one's role in a community.[74] For this reason, Confucius defined *ren* in different manners depending on the person asking the questions. Modern Confucius scholars have given new interpretations to many of Confucius' works. For example, Tu[75] extends his interpretation to include ecological issues, O'Dwyer[76] to include democracy, and Tsai[77] to include bioethics. Similarly, extension of duties beyond the classic five relationships has also been newly interpreted. It could be said that certain members of society may have the duty to disclose information on epidemics which could save lives, reduce the spread of the infectious disease, and perhaps altogether avoid a disease reaching the level of epidemic. It could equally be said that certain members of society may feel morally obliged to unveil what types of information is censored, how the information is censored, and methods including anonymity networks as part of an anti-censorship strategy. Certain societal members may include scholars, doctors, journalist, experts, NGOs, and other international organizations. This bears a resemblance to justifications of the moral agent in conscientious disobedience. The disclosure of censored information, and the dissemination of vital information is potentially a virtuous act whether it is through direct means of an Internet website, news publications, or whether it is less direct through a benevolent worm.

WILL THE BOAT SINK THE WATER?[78]

Water holds up the boat;
Water may also sink the boat.

Emperor Taizong (600-649, Tang Dynasty)

In much the same way, benevolent payloads have the potential to be destructive. They also have the potential to be beneficial. Benevolent payloads have in the past been analysed in the context of patches and e-commerce. Conclusion has been reached in the wider technological community that benevolent payloads are simply a 'bad idea' because

[74] Chan, J. (2002) Moral Autonomy, Civil Liberties and Confucianism. Philosophy East and West. 52,3.
[75] Tu, W-M. (1985) Confucian thought: selfhood as creative transformation. State University of New York Press, New York. See also Tu, W-M. (1993) Way, Learning, and Politics: Essays on the Confucian intellectual. Suny.
[76] O'Dwyer, S. (2003) Democracy and Confucian Values. Philosophy East and West, 53, 1, 39-63.
[77] Tsai, D. (2005) The bioethical principles and Confucius' moral philosophy. Journal of Medical Ethics, 31
[78] The title of a book banned in China. Guidi, C. and Chuntao, W. (2006) Will the Boat Sink the Water? Public Affairs, Perseus Books Group, USA.

there is no consent, and there are safer methods available. There has been no analysis of benevolent payloads outside of the electronic commerce context. A benevolent worm performing anti-censorship tasks provides an interesting case study which undermines and challenges many of the ethical issues of benevolent payloads. This article has attempted to untangle many of the complex ethical and legal issues surrounding benevolent payloads.

BIOGRAPHY

Alana Maurushat, B.A. (University of Calgary), B.C.L.(McGill), LL.B. (McGill), LL.M. with Concentration in Law and Technology (University of Ottawa), PhD Candidate (University of New South Wales). The author Deputy Director of the Cyberspace Law and Policy Centre, part-time lecturer, and PhD candidate at the Faculty of Law, UNSW. Prior to moving to Sydney, she was an Assistant Professor and Deputy Director of the LLM in Information Technology and Intellectual Property at the University of Hong Kong's Faculty of Law. She has taught in summer programs for the University of Santa Clara, Duke University, and has been invited to teach at the Université de Nantes this coming year. Her current research is focused on technical, ethical and legal dimensions of computer malware building on past research projects which addressed the impact of surveillance technologies on free expression and privacy.