Potential of ICTs for Conflict

Fall 2010, markus.sabadello@gmail.com

Contents

1. Introduction

Information and Communication Technologies (ICTs) have greatly transformed societies, cultures and economies as well as created both new opportunities and threats for humankind. Since at least Manuel Castells' widely cited book trilogy "The Information Age"[1], we have a good scientific understanding of the causes, nature and consequences of today's interconnected society that is the result of the spreading of ICTs and the globalization processes accompanying them. And since at least the World Summit on the Information Society[2], which culminated in its second phase in 2005 in Tunis, the United Nations as well as a large amount of other stakeholders have been working on evaluating the potential of ICTs for the values of peace and democracy, as well as the risks of conflict and abuse caused by such technologies.

Following Sigmund Freud's concept of the two forces *Eros* and *Thanatos* – a drive for creation and a drive for destruction which both live in all of us, the Internet has often been described as a neutral tool which can be used for good or evil, just like a hammer can be used to build a house or to murder a person. When the Internet became widely available in mainstream society during the 1990s, the fast spreading of this then new technology sparked strong reactions on both ends of the spectrum, ranging from utopist hopes that new levels of democracy and transparency would lead to a more peaceful and just world, to the fear that its effects on humanity would threaten political and social orders world-wide.

Such ambiguous responses have always been typical of new technological developments in human history. The invention of railroads has led to concerns about the "annihilation of space and time" and its adverse effects on the human psyche[3]. During Japan's Meiji Restoration in 1868, violent conflict emerged in response to plans to drastically modernize the country. In Hollywood movies such as "*Tron"* (1982), *"The Terminator"* (1984) or *"I, Robot"* (2004), the central narratives are based on the fear of new technology. The invention of the telegraph in the 1800s, its deployment throughout the United States, and the first transatlantic cable led to hopes that a technology which

[1] See (Castells, 2000)

[2] See http://www.itu.int/wsis/

[3] See (Lardner, 1850) for an early assessment of the effects of railroad travel.

allowed people and governments all over the world to send and receive messages at instant speed would lead to an end of old prejudices, to universal understanding and peace – a vision strikingly similar to that of today's Internet utopists[4]. All these historical developments have one thing in common: Strong reactions to fast change introduced by technological advance. In order to truly judge both the opportunities and dangers of today's ubiquitous ICTs, it is important to try to maintain realism and objectivity and to keep in mind that technology can always be used for good or evil.

On the positive side – which I have tried to analyze in my recent paper "Potential of ICTs for Peace" – it can be used as a tool by international organizations and NGOs to perform their work more effectively. It can be used as a weapon in nonviolent struggle to fight for a legitimate political goal. It can also act as a means for intercultural dialogue, to promote understanding, and as a pillar of peaceful societies. In this paper, I will now attempt to more closely examine the opposite side of the same coin, i.e. the various ways in which ICTs can lead to harm and conflict. The motivation for this endeavor is that in the best tradition of the militaristic virtue of "knowing your enemy", we as peace researchers and activists must understand the dangers of ICTs before we can rightly claim to understand their possible use for good.

2. Properties of the Medium

In order to explore the potential of the Internet and other ICTs for peace and conflict, it appears necessary to first examine at least on a basic level the characteristics and abilities of electronic communication technologies that can act as a medium for exchanging information between senders and receivers.

From a high-level point of view, the Internet's principal differences from more traditional media are its high speed, low price and interactivity. Extensive academic work has been done to describe mathematical aspects of electronic communication technologies, such as reliability, latency, or the amount of information that can be transmitted over a channel in a given amount of time. In his influential work "The Mathematical Theory of Communication"[5], Claude Shannon – generally considered one

[4] See (Standage, 1999) for a comparison of hopes and fears in reaction to the introduction of the telegraph and the Internet.

[5] See (Shannon & Weaver, 1963)

of the founding fathers of information and communication theory – defines several key concepts of communication, such as sender, receiver, message, channel and "bit" as a mathematical unit for measuring information. Building on this foundation, it becomes possible to evaluate the potential of various electronic communication technologies for transmitting information.

It is important to point out that this mathematical notion of information is related to, but quite distinct from the human-understandable semantics that are being exchanged in human communication. It is self-evident that the form of communication most capable of conveying human-understandable semantics is direct face-to-face communication, which besides words also consists of important nonverbal components, such as tone of voice, facial expressions, body gestures, eye contact, physical contact and others. According to estimations, nonverbal communication accounts for 60 to 70 percent of human-understandable semantics. Compared to face-to-face communication, any electronic medium is necessarily more limited and less able to efficiently convey all the semantics that are typically found between humans. Electronic communication technologies come in many different forms, from text-based telegraph systems to modern multimedia applications. In general, an increased ability to transport information in the mathematical sense of Claude Shannon (i.e. a high "bitrate") also results in an increased potential to convey human-understandable semantics, however due to their variety it is still necessary to examine all the different concrete applications of ICTs individually. Sometimes, limited technologies such as text-based systems can be semantically enhanced in creative ways, such as by spatial arrangement of words or the use of emoticons.

Georg Simmel defines variables such as "self involved" and "distance"[6]. Although he uses them primarily to examine conflict as a social form, it seems his approach can also be suitable for judging the potential of various ways of communication for conveying human-understandable semantics. The main lessons to be kept in mind here about the Internet as a medium are that 1. It is fundamentally different from previous media in various ways, and that 2. Different applications on the Internet can exhibit significantly

[6] See (Simmel, 1971)

different communication characteristics and as a result, different potential for social effects.

3. Information Overload and the Digital Divide

Information Overload is a term that was coined before ICTs played a role as a mass medium and refers to a situation of being overwhelmed with too much information to handle[7]. It was originally used to describe technological change in general and has gained new relevance with the advent of the Internet on a large scale. One of the most-often cited advantages of the Internet – the possibility to quickly access a huge amount of information – is therefore put into question and turned into a negative concept. Information, which is traditionally seen as something positive, can become a problem in itself if available in amounts too large to process and in a structure too hard to search. As Herbert Simon puts it, *"A wealth of information creates a poverty of attention"*[8].

To some extent it is possible to adapt to this problem after some time of learning, but this ability varies from individual to individual by factors such as age, social status, cultural background and experience. Technologies exist to deal with overwhelming amounts of information, like search engines or attempts to introduce structure into the web[9], however care must be taken not to restrict the universality and openness of the Internet or to introduce cultural bias when organizing information.

Another well-known problem associated with the widespread availability of information and communication possibilities introduced by the Internet is the so-called "Digital Divide" (or "Digital Gap"), which is the unequal ability among people to access ICTs, both between different areas of the world and among different parts of society within a country. The Digital Divide is caused to a large part by unequal levels of availability of the technical ICT infrastructure, but also by differences in education and "computer literacy" – the skills required to efficiently use ICTs. The existence of such differences results in disadvantages of those groups of people who do not have adequate access to

[7] This term was popularized in (Toffler, 1970), which discusses social effects of change that happens too fast.

[8] See (Simon, 1971)

[9] For example, the „Semantic Web" is a set of efforts and technologies aimed at making information more machine-readable and thus organize it in ways that make it easier for humans to consume.

ICTs and therefore cannot fully benefit from their potential. Therefore, ICTs can not only serve to help solve some of world's big challenges, but can in fact result in new problems as well as in the amplification of existing ones.

4. Cyberwarfare, Cyberterrorism and Cybercrime

These terms refer to the use of ICTs as instruments in warfare, terrorism and criminal activities. Exact definitions of warfare and terrorism are hereby left out due to the complexity of these concepts, but generally involve organized, violent action for the purpose of advancing a political agenda. Cyberwarfare and cyberterrorism are based on the realization that political, social and economic systems world-wide have come to heavily depend on ICTs. Therefore, significant harm can be inflicted to an enemy by attacking its ICT infrastructure.

It should be pointed out that warfare conducted via online technologies is in many ways different from all other forms of warfare that have existed in human history[10]. Traditionally, the most important assets for defeating one's enemies have always been strength, space, time and knowledge of the enemy, with the last item on this list being the most important. Also, on traditional battlefields, it was always the defender who had an advantage, because of their better familiarity with terrain and potential threats. When it comes to computer systems and communication networks however, none of these principles hold true anymore. In this new type of warfare, strength, space, time and especially knowledge have completely new meanings, and in case of an attack, a defender is clearly disadvantaged because of a large number of different, unpredictable threats that could arise from anywhere at any time. Other aspects of traditional warfare however are still valid in the online world, for example the concentration of resources when conducting an attack, and the concept of preemptive strikes. On this battleground, the offensive weapons are hacking activities, viruses and denial-of-service attacks, while the defenses center on firewalls, redundancy and intrusion detection.

On the most basic level, cyberwarfare and cyberterrorism can be employed to attack computer systems that are directly connected to the Internet and publicly accessible.

[10] According to (The Economist, 2010), cyberspace should be considered a "fifth domain" of warfare after land, sea, air and space.

The potential damage that can be inflicted ranges from disabling the operations of companies, Internet service providers and individual Internet users, to the impairment of the Internet structures of entire countries. However, given the amount of use of ICTs throughout all aspects of societies and economies, potential attack targets go far beyond those systems that are publicly connected to the Internet and can include vital infrastructure such as power grids and other industrial facilities, financial institutions, road and air traffic control systems, and hospitals. Subtypes of cyberwarfare and cyberterrorism include electronic espionage, the use of hacking techniques for disabling an enemy's electronic weapon systems in order to facilitate a conventional attack, and the integration of high-tech ICTs into existing and new weapons system such as unmanned aerial drones.

Since these types of attack are relatively new and involve a lot of uncertainty, fears about an impending "digital Pearl Harbor" or "cybergeddon" have been raised[11]. One should be careful not to overstate the threat posed by cyberwarfare and cyberterrorism, especially in relation to other serious problems the world is facing, but such attacks do have the theoretical potential to inflict serious damage and even human casualties to an enemy. Militaries around the world have recognized the need for cyberwarfare strategies and have developed both offensive and defensive capabilities to attack an enemy's online infrastructure as well as to protect one's own. Examples include USCYBERCOM[12] (a command of the U.S. armed forces), and the "Elektronische Abwehr" (German for "electronic defense") of the Austrian Army.

Although cyberwarfare has not yet received a large amount of public attention, events have happened that fall into this category, for example:

- In 1982, during the Cold War, the CIA succeeded in manipulating the software of a Soviet gas pipeline, reconfiguring the technical parameters of pumps and valves to the point where the pipeline was disabled by an explosion[13].

[11] See (Knake & Clarke, 2010) for an introduction and description of possible scenarios.

[12] It is interesting to note that USCYBERCOM's mission is only to defend military networks, while the responsibility to protect civil ICT resources lies within a different institution, the U.S. Department of Homeland Security.

[13] See (Murphy, 2010)

- In 1998 during the US and NATO attacks on Serbia, Serbian air defense systems were hacked in order to perform conventional aerial attacks more effectively[14].
- In 2007, websites of Estonian governmental institutions and companies were hit by denial-of-service attacks to the point where they were no long able to respond to legitimate requests. The result of this incident was significant financial effort required to repair the damage, as well as a sudden increase of global consciousness about this kind of threat[15].
- In 2011, the Stuxnet virus – perhaps the most famous example of cyberwarfare to this date – caused severe damage to nuclear facilities in Iran and other countries. This attack was noteworthy because it was custom-tailored to attack a very specific kind of target (namely, Siemens industrial equipment), and because due to the re-programming of such equipment it has resulted in actual physical damage, effectively demonstrating to the world the threat from cyberwarfare[16].

Cybercrime is similar to cyberwarfare and cyberterrorism in that its actors also attempt to exploit the high level of dependency on ICTs that many of us experience in our lives. However, just like crime is generally treated very differently from warfare and terrorism in that it is aimed at personal gain rather than political goals, cybercrime should also be considered a separate problem in which ICTs can cause conflict and harm to individuals. While the technical methods may be similar, the goal of cybercrime is often not so much the infliction of damage to an enemy, but the illegal accumulation of financial wealth. One term that has been popularized in the context of cybercrime is "identity theft", which is a type of criminal activities to take over an individual's online identity for the purpose of stealing sensitive, valuable information or even hijacking bank accounts and making unauthorized payments.

5. Data Mining

Data mining refers to methods and technologies aimed at extracting useful patterns from the data individuals produce as they use online services. With every step we take on the Internet, every piece of information we type on the screen, every mouse click we

[14] See (Arquilla, 2003)

[15] For example, see (Traynor, 2007)

[16] For example, see (Beaumont, 2010)

perform, we are adding more data to our online identity, our digital fingerprint. Just like in other cases discussed in this paper, the process of data mining can be used either for the advantage or disadvantage of individuals. On the positive side, sophisticated programming based on our data can help us customize the services we use, provide for a better overall online experience and potentially even mitigate the challenges posed to us by Information Overload (see section 3). On the negative side, there is a vast amount of potential abuse by those companies in control of our data, which can range from direct monetization of our information by the means of targeted advertising, to the conscious and malicious manipulation of what we see and do online, leading to influence on our consumption behavior and political views.

The amount of data that is being collected and analyzed is typically much larger than the average individual would expect. The perceived freedom and user-centricity that seem to be inherent to the way we have been educated to use the Internet can all too easily hide the fact that between individuals and companies, there is almost always a huge imbalance of control over data in favor of the latter. An entire industry has emerged that has specialized in developing technologies for data collection and data mining. One example company out of many in this industry is Wakoopa[17], which states that its software *"creates digital DNA of today's consumer"* and *"analyzes data and optimizes your digital strategy"*. Another example is the well-funded and often criticized company Phorm[18], which produces software that is being used by Internet Service Providers all around the world today to analyze the entirety of data sent and received by their users.

All of the largest and most popular Internet companies – such as Google, Facebook, Twitter and Youtube – are based on the idea of offering supposedly "free" services in exchange for collecting and monetizing valuable data about their users[19]. In a hearing conducted by a subcommittee of the U.S. House of Representatives in 2010, Prof. Eben Moglen of the Columbia University Law School states that *"Facebook holds and controls more data about the daily lives and social interactions of half a billion people than 20th-century totalitarian governments ever managed to collect about the people they surveilled"*.

[17] See http://wakoopa.com/

[18] See http://phorm.com/

[19] For a discussion on hidden costs behind seemingly "free" services, see (Krotoski, 2010)

When looking at the practices of such companies, the transparency as well as the possibilities to control the use of personal data are typically minimal. Facebook in particular – but others as well – have often been criticized for lack of information on what kind of data is being collected and how it is used. In fact, senior executives of such companies seem to do little to hide the fact that their business models are based on treating their users' data in very liberal ways.

For example, Facebook CEO Mark Zuckerberg states in an interview[20] that *"People have really gotten comfortable not only sharing more information and different kinds, but more openly and with different people. That social norm is just something that has evolved over time"*. Similarly, Google CEO Eric Schmidt states in an interview[21] that *"If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place"*.

The ideas about privacy suggested in such statements by top representatives of leading Internet companies are unlikely to resonate well with the majority of their users. The realization that unbounded collection of data and the application of data mining techniques are often not in the best interest of users is old and has resulted in a number of initiatives to protect individuals' privacy. Such protection can be achieved in two ways: On one hand, through political guidelines and legislation – such as the *Data Protection Directive* of the European Union (Directive 95/46/EC), the *Privacy Framework* of the Asia-Pacific Economic Cooperation (APEC), OECD's *Guidelines on the Protection of Privacy*, or the *Fair Information Practice Principles* of the U.S. Federal Trade Commission.

On the other hand, privacy and thus less vulnerability to the adverse effects of data mining can also be achieved through technological means. Software solutions such as proxy servers, privacy plugins for web browsers or anonymizing peer-to-peer networks can greatly reduce the amount of personal data that is exposed as we use Internet services. Just like there is an industry specializing in exploiting the wealth of personal data on the Internet, there are also initiatives aimed at protecting privacy. Examples

[20] See http://www.ustream.tv/recorded/3848950

[21] See http://www.youtube.com/watch?v=A6e7wfDHzew

include the UK-based community interest company Mydex[22], whose mission is to *"help individuals realize the value of personal data"*, or personal.com, which claims to allow you to *"decide who gets access to your data and time"*.

The conflict between the desire for privacy as a fundamental human right[23], and a commercial incentive for companies to gather information about their existing and potential customers is much older than the Internet, but has proven to be more relevant than ever before in a world that is increasingly more connected and open. With the increasing use of online service on phones and other mobile devices and the data that is generated by such use[24], this trend will continue and accelerate.

6. Cultural Conflicts

Another important aspect of ICTs (and especially the globalization processes that have been accompanying them) is their impact on cultures and social systems. In the best tradition of Marshall McLuhan, who famously stated that *"the medium is the message"*, the very way in which we use ICTs has already considerably altered our ways of life and the way in which we relate to technology. Beyond such basic realizations about our own behavior, the fact that technology has led to a highly interconnected world has in turn also resulted in new ways in which cultures cooperate, compete and otherwise interact with each other. Throughout history, cultures have emerged, disappeared and transformed because of the ability – or lack thereof – to communicate with other people and exchange aspects of one's identity with others. With the Internet, such processes have gained an additional medium and new dynamics. Some scholars such as Nicholas Negroponte[25] argue that ICTs will have such a profound impact on cultures and societies to the point where *"the net will abolish the nation-state"*, however as usual one should be careful not to overstate the potential of technology.

---

[22] See http://www.mydex.org/. A community interest company is a legal entity that is audited and regulated to use its assets for public good.

[23] See Article 12 of (United Nations, 1948)

[24] For example, see the „Reality Mining" project by the MIT Media Lab, which is aimed at collecting and mining data from individuals' cell phones: http://reality.media.mit.edu/

[25] Nicholas Negroponte is founder of the MIT Media Lab and known for his blog "Being Digital" as well as for the One Laptop Per Child initiative.

On the positive side, ICTs can be an asset for intercultural dialogue and for overcoming cultural differences, a topic which UNESCO is most involved with, famously stating in its constitution that *"Since wars begin in the minds of men, it is in the minds of men that the defenses of peace must be constructed"*. In 1990, after recognizing the potential behind ICTs for its goals, UNESCO established the operational sector "Communication and Information", which since then has become of equal importance as the three classic sectors "Education", "Science" and "Culture".

On the negative side, ICTs can also intensify competition and conflict between cultures. According to Samuel P. Huntington and Geert Hofstede, cultural and religious identities are major sources for conflict[26], and *"culture is more often a source of conflict than of synergy"*[27]. ICTs offer new weapons for conducting today's and future cultural and religious conflicts, for example, Evgeny Morozov states that *"if you had to choose one weapon for fighting the next religious war, you could do worse than to pick an iPhone"*[28].

7. Political Movements

ICTs have often been said to offer large potential when it comes to nonviolent struggle and popular movements working towards values such as democracy and social justice. This idea is rooted in one of the most basic properties of this medium – its interactivity, which allows individuals to be both producers and consumers of information, to exchange thoughts and organize themselves. Modern popular movements often involve using the Internet both as an organizational tool and as a medium for disseminating their political messages to the public. For example, the Internet has been used effectively in the following cases:

- Mexican Zapatista Army of National Liberation (EZLN): Having been called the "first informational guerilla movement", the EZLN has pioneered the idea of building a world-wide network of supporters through the effective use of media[29].

[26] See (Huntington, 1996)

[27] See (Hofstede, 2001)

[28] See (Morozov, God Bless This Gadget, 2009)

[29] See (Castells, 1997)

- Otpor!: In 2000, the successful Serbian nonviolent movement against the socialist regime of Slobodan Milošević had a website for publishing their political messages, before it even had an office[30].
- Colombian Anti-FARC protests: Hundreds of thousands of people in Bogotá held a march in February 2008 to protest the violent activities of FARC. This event was organized to a large part via Facebook[31].
- Iran Green Revolution: In this civil rights struggle following the controversial presidential election in 2009, Facebook, Twitter and blogs were used to organize the movement and to spread information to members and international supporters[32].
- Tunisian Jasmine Revolution: After decades under the rule of President Zine El Abidine Ben Ali, a popular uprising sparked in 2010 by continuing unemployment, oppression and despair, has forced the President and his wife to flee the country. In a similar manner to Iran, Facebook and Twitter were used to organize the protests and to attract supporters.
- Egypt Protests: Inspired by the events in Tunisia, a similar popular movement has emerged in 2011 in Egypt, also calling for social reforms and the removal from power of the country's leader Hosni Mubarak.

The widespread use of social networking services on the Internet in the above mentioned political movements has led to the popularization of the term "Twitter Revolution"[33], which however appears to be a poor choice, because it hides the true nature of a movement and its intentions. Rather than emphasizing the political cause or the character of the movement's principals, it emphasizes a technical tool, which can lead to false hopes and expectations that sometimes go hand in hand with an unrealistic allure of modern technologies. Nevertheless, despite the ill-chosen term and some misconceptions around it, the use of the Internet has without doubt played an important, positive role by accelerating and amplifying movements such as the protests in Tunisia and Egypt – and more may follow.

---

[30] See (York, 2002)

[31] See (BBC NEWS, 2008)

[32] See (The Washington Times, 2009)

[33] And derivatives (e.g. "Wikileaks Revolution")

One important and inevitable aspect of the use of the Internet and other media in revolutionary political movements is that access to them is naturally not limited to members and supporters of such movements, but also available to their opponents in at least the same way. Historically, attempts by established authorities to control and manipulate communication technologies have a long tradition, from the Catholic Church's early attempts to control Gutenberg's printing technology to the fearsome propaganda machine of German National Socialism. Today, movements that are directed against an established governmental authority will often find themselves confronted with an imbalance of power not only in the form of control over traditional media, the police force, the army and other institutions, but also on the Internet, which governments can easily monitor, analyze, manipulate, slow down or turn off altogether. There are technical approaches to circumventing such obstructive measures, for example anonymizing proxy servers, alternative DNS root name servers and private alternative network devices. However, ultimate control over Internet infrastructure always lies within a country's major telecommunication companies, and with the state.

In Tunisia, censorship of traditional media as well as of the Internet has existed well before the beginning of the protests. All control over the Internet is centralized within the government, which has not hesitated to filter and shut down websites at will[34]. In Egypt, where the political situation is comparable, the regime has even gone as far as blocking Internet access entirely[35], both for domestic users and for incoming international requests, which is a move that is unprecedented in Internet history. Reportedly, the regime has even banned the popular news network Al-Jazeera, because of its reputation of being supportive of popular movements in the Arab world by covering them in open and unrestrictive ways[36]. The rationale behind such measures is clear: Movements relying on the Internet for organization and public outreach can be hurt by simply disabling the infrastructure which they are based on. Mohamed El Baradei – former Director General of the IAEA and speculated to perhaps taking a major role in a future new Egyptian government – has said that *"Unfortunately, I have to get out of Egypt, to be able to speak about the plight of the Egyptians"*.

---

[34] For example, see http://anarcat.koumbit.org/censuretunisie

[35] See (Kanally, 2011)

[36] See (Al Jazeera, 2011)

Even in the United States with its self-image of defending democracy and civil liberties, a law[37] has been introduced which theoretically allows the president to directly take control of Internet infrastructure in the event of a "national emergency".

Apart from censorship of ICT infrastructure, popular movements relying on the Internet may also face other difficulties, as was demonstrated by the failure of the Iran Green Revolution to quickly achieve its goals. Just like the technology can be used by protesters to disseminate their political positions and to organize themselves, it can equally be used in the same ways by their opponents in the political establishment, for example to undermine the movement's outreach efforts, or to monitor and then effectively combat its organizational structure, which can be as simple as taking a look at suspected activists' Facebook pages or the lists of their followers on Twitter. Evgeny Morozov – coining terms such as "digital dictatorship" and "splinternet" – suggests that the Internet may actually be more useful to authoritarian regimes than to the popular movements that oppose them. He argues that the reason for the Soviet Union to collapse was inferior information about what was going on in the country, and that the Berlin Wall might still be standing, had Twitter existed earlier and alerted the government of East Germany of the hate felt by its population. He also mentions Chinese bloggers who are paid by the government to publish favorable statements about the established political system – an example confirming that the ability for ICTs to spread political views is available to all sides of ideological conflicts[38].

A further concern related to the use of ICTs in popular movements include the realization that Facebook, Twitter, Youtube and similar services might over time function more and more as an extension of the U.S. state and a tool of its foreign policy and diplomatic efforts[39], leading to a form of cultural hegemony or imperialism, rather than being independent and completely neutral technologies[40]. Also, from a technical

---

[37] See (Sen Lieberman, 2010)

[38] See (Morozov, The Digital Dictatorship, 2010) for a discussion on how the Internet may be more useful to authoritarian regimes than to their opposing popular movements.

[39] For example, see http://www.state.gov/m/irm/ediplomacy/, the U.S. State Department's "Office of eDiplomacy".

[40] The term „Twitter Diplomacy" has been coined for this idea. See (Lee, 2011) and (Morozov, The Digital Dictatorship, 2010)

perspective, most major Internet services have in terms of their structure much more in common with authoritarian regimes than with movements that are directed against them. Although the participants of so-called “Twitter Revolutions” may be driven by egalitarian and democratic values, the online services they use are run by centralized, profit-oriented and often secretive corporations, rather than being organized in a democratic and transparent fashion – a fact that is all too easily overlooked and forgotten.

The discussion on what role the Internet can actually play to bring freedom to the world is therefore unresolved.

8. Conclusions

The following table summarizes some of the discussed effects of ICTs on peace and conflict, grouped by high-level categories. The main conclusion of this paper is a pattern of symmetry, i.e. it can be noted that for most positive uses of ICTs leading to the values of peace and democracy, there are also matching negative uses that can lead to harm and conflict:

Potential of ICTs for Peace	**Potential of ICTs for Conflict**
Basic access to information via ICTs	
• Use of ICTs for capacity building, i.e. empowering disadvantaged people to help themselves through access to information • Use of ICTs for education	• Information Overload • Digital Divide
Use of ICTs as an organizational asset	
• Use of ICTs by political movements to organize themselves as well as their supporters • Use of ICTs by International Organizations and NGOs to perform their work more effectively, e.g. to improve internal, administrative processes, to organize disaster relief operations, etc.	• Use of ICTs as an organizational asset by terrorist groups, e.g. to coordinate attacks • Use of ICTs by authoritarian regimes to analyze and combat the organizational structure of oppositional movements

Use of ICTs as a political communications channel	
• Use of ICTs in nonviolent struggle to publish political messages and attract supporters	• Use of ICTs by terrorist groups and authoritarian regimes to publish political messages and attract supporters • Use of ICTs by authoritarian regimes for propaganda
Ubiquity of ICT infrastructure	
• Making many everyday tasks easier to perform, and meeting basic communication needs	• Data Mining • Cyberwarfare, Cyberterrorism and Cybercrime
Social and cultural impact of ICTs	
• Intercultural dialogue • Building and maintaining peaceful societies	• Globalization of culture • Use of ICTs in cultural and religious conflicts

Ultimately, when judging the potential of ICTs for peace and conflict – which is a discussion that will continue and intensify in the future – it is important to remain objective, to neither become subject to extreme techno-utopianism that hails ICTs as a panacea for all of the world's problems, nor to demonize the change that always comes with new innovation. It is also important to keep in mind that ICTs can always only be one part of a solution to a conflict, rather than miraculously solving problems without much effort, which is an occasional perception reminiscent of the old concepts of "opium for the masses" and "panem and circenses".

In the struggle between the ancient forces of *Eros* and *Thanatos* that are now applied to the modern ICT context, peace researchers, activists and technologists alike are called

upon to employ their efforts to work towards maximizing the potential of ICTs for peace and democracy, while at the same time trying to minimize their opposite potential for harm and conflict.

9. Bibliography

Al Jazeera. (30. January 2011). *Egypt shuts down Al Jazeera bureau*. Von Al Jazeera: http://english.aljazeera.net/news/middleeast/2011/01/201113085252994161.html abgerufen

Arquilla, J. (2003, March 4). *Interview: John Arquilla.* Retrieved from Frontline: Cyber War!: http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html

BBC NEWS. (2008, February 4). *Colombians in huge Farc protest .* Retrieved from BBC NEWS: http://news.bbc.co.uk/2/hi/americas/7225824.stm

Beaumont, C. (2010, September 23). *Stuxnet virus.* Retrieved from The Telegraph: http://www.telegraph.co.uk/technology/news/8021102/Stuxnet-virus-worm-could-be-aimed-at-high-profile-Iranian-targets.html

Castells, M. (1997). *The Information Age: Economy, Society and Culture: The Power of Identity* (Vol. 2). Oxford: Backwell.

Castells, M. (2000). *The Information Age: Economy, Society and Culture: The Rise of the Network Society* (2 ed., Vol. 1). Cambridge, MA.

Hofstede, G. (2001). *Culture's Consequences: Comparing Values, Behaviors, Institutions,.* Thousand Oaks, CA: SAGE Publications.

Huntington, S. (1996). *The Clash of Civilizations and the Remaking of World Order.* New York: Simon & Schuster.

Kanally, C. (2011, January 27). *Egypt's Internet Shut Down*. Retrieved from The Huffington Post: http://www.huffingtonpost.com/2011/01/27/egypt-internet-goes-down-_n_815156.html

Knake, R., & Clarke, R. (2010). *Cyber War.* Ecco.

Krotoski, A. (2010, February 12). *Virtual Revolution: The Cost of Free.* Retrieved from The Guardian: http://www.guardian.co.uk/technology/blog/2010/feb/12/virtual-revolution-bbc-aleks-krotoski

Lardner, D. (1850). *Railway Economy.* London.

Lee, M. (2011, January 23). *Twitter Diplomacy*. Retrieved from The Huffington Post: http://www.huffingtonpost.com/2011/01/23/twitter-diplomacy-us-dipl_n_812830.html

Morozov, E. (2009, July 18). *God Bless This Gadget.* Retrieved from Newsweek: http://www.newsweek.com/2009/07/17/god-bless-this-gadget.html

Morozov, E. (2010, February 20). *The Digital Dictatorship*. Retrieved from http://online.wsj.com/article/SB10001424052748703983004575073911147404540.html and http://www.youtube.com/watch?v=i4U_fqAZE2g

Murphy, M. (2010, July 1). *War in the fifth domain*. Retrieved from The Economist: http://www.economist.com/node/16478792

Sen Lieberman, J. (2010). *Protecting Cyberspace as a National Asset Act.* The Library of Congress.

Shannon, C., & Weaver, W. (1963). *The Mathematical Theory of Communication.* Urbana, IL: University of Illinois Press.

Simmel, G. (1971). *On Individual and Social Form.* (D. Levine, Hrsg.) Chicago, IL: University of Chicago PRess.

Simon, H. (1971). Designing Organizations for an Information-Rich World. In M. Greenberger, *Computers, Communication, and the Public Interest.* Baltimore: The Johns Hopkins Press.

Standage, T. (1999). *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-line Pioneers.* New York: Walker and Company.

The Economist. (2010, July 1). *War in the fifth domain.* Retrieved from The Economist: http://www.economist.com/node/16478792

The Washington Times. (2009, June 16). *EDITORIAL: Iran's Twitter revolution.* Retrieved from The Washington Times:

http://www.washingtontimes.com/news/2009/jun/16/irans-twitter-revolution/

Toffler, A. (1970). *Future Shock.* New York: Random House.

Traynor, I. (2007, May 17). *Russia accused of unleashing cyberwar to disable Estonia.* Retrieved from The Guardian: http://www.guardian.co.uk/world/2007/may/17/topstories3.russia

United Nations. (1948). *Universal Declaration of Human Rights.* Retrieved from http://www.un.org/Overview/rights.html

York, S. (Director). (2002). *Bringing Down a Dictator* [Motion Picture].