Scenarios: ICTs for Peace and Conflict in 2020

Spring 2011, markus.sabadello@gmail.com

Contents

1. Introduction

The widespread availability of Information and Communication Technologies (ICTs) has led to the globalization process and continues to have a large influence on social, economic, political and cultural structures around the world. Much work has been done in the academia to get to a good scientific understanding of the causes, nature and consequences of today's interconnected world[1], and to analyze both opportunities and threats that ICTs pose to humankind. In the context of Peace and Conflict Studies, ICTs can play an important role in many ways. On the positive side, communication technologies such as the Internet can support nonviolent, democratic movements, promote education, capacity building, intercultural dialogue and the establishment of a beneficial global civil society. They can also play a liberating role in processes to overcome authoritarian regimes, as has been demonstrated by the recent revolutions in the Arab world[2]. On the negative side, ICTs can be used for cybercrime, cyberwarfare, surveillance, the spreading of extremist propaganda, the suppression of democratic processes and other destructive purposes.

This paper is an attempt to apply the Scenario Building technique to consider the role that ICTs might have for peace and conflict in the year 2020. This chosen topic is especially challenging for two reasons: First, hardly any field moves as fast as modern ICTs. The speed and unpredictability of achievements in computer technology and the Internet have again and again astonished both the general public and professional analysts. Second, when trying to make statements about the future role of technology, there is always a general tendency to emotional debate and to overstating their influence. For example, with the introduction of the telegraph 200 years ago, as well as with the introduction of the communications satellite 50 years ago, there was a general sense that such technologies would overcome barriers of space and time, and therefore enable all peoples of the world to communicate with each other at a new level, which would avoid conflicts altogether and lead to a perpetual peace. This is a vision that is now again popular among today's Internet utopists, however, the reality remains that in

[1] For example, see (Castells, 2000)

[2] The term sometimes used for these movements – "Twitter Revolution" – is of course an exaggeration, but still illustrates the importance of modern ICTs in political discourse and conflict.

our present time we continue to face a large amount of conflicts and other challenges. Therefore, even though the idea of Scenario Building is to be creative when considering possible developments, a basic sense of realism must be preserved.

The goal of this paper is explicitly to consider ICTs in the particular context of Peace and Conflict Studies rather than their general future, which would be much too wide. One central element in this endeavor will be the ongoing securitization process that can be observed when it comes to ICTs. From monitoring and censoring of online communication in states such as China, to the rise of cyberwarfare, to the idea that Facebook, Twitter, Youtube & Co can be used as diplomatic instruments for maintaining Western hegemony in the world[3], the discourse around ICTs is increasingly shaped by the portrayal of these technologies as threats. While a general discussion about regulation and the unavoidable tradeoff between freedom and security on the Internet is not new, high-level discourses about its influence on societal and political security are now taking place and gaining in rhetorical harshness and emotional involvement from all sides.

During the Scenario Building process, possible driving forces will be identified that are likely to have a more or less strong influence on the development of ICTs and their potential for peace and conflict. At the end of the process, a set of four possible stories about the future will be developed, however without claiming objectivity or completeness, and without making statements about the probabilities of each story coming true.

[3] For example, see (Mann, 2011)

2. List of Driving Forces

As the first step in the Scenario Building process, this section will try to identify a number of actors and driving forces that are likely to influence to a more or less extent the evolution of the role ICTs will play in 2020 for peace and conflict.

Driving Force	Explanation
Internet Users	The group of all individuals using the Internet is large and diverse, but shares a few common interests, e.g. the desire that the Internet services they use always work well.
Internet Service Providers	The companies providing Internet services have a commercial interest in their customer's money and are therefore likely to offer whatever the market demands, limited by the legal frameworks they are operating in.
Revolutionary Movements	Revolutionary movements such as the Iranian Green Movement of 2009, the Tunisian "Jasmine" revolution of 2011, or the Egyptian revolution of 2011, use ICTs as a powerful tool for self-organization as well as for political outreach.
Authoritarian States	Given the important role ICTs have played in several popular uprisings, authoritarian states are likely to 1. Try to limit the potential of ICTs for such movements, and 2. Try to use them for their own purposes, e.g. propaganda and surveillance.
Democratic States	While the access to information and freedom of expression are commonly accepted fundamental rights within democracies, such states are also exhibiting trends to increase their ability to control and monitor ICTs[4].
Universities	Technical academic disciplines such as electrical engineering and computer science have always been at the forefront of advancing

[4] For example, see the Data Retention Directive (Directive 2006/24/EC) of the European Parliament and Council.

	the development of ICTs. Social sciences on the other hand aim at analyzing and reflecting upon the effects of ICTs on societies. Researchers and students at academic institutions will continue to have an influence both on the development of new technology and on studying their consequences.
Think Tanks	Think Tanks try to predict the evolution of ICTs and their effects on society. Their work is often based on specific political or economic interests.
Globalization	The process of globalization continues to both influence and be influenced by the invention of new ICT services.
Internet Governance	While the Internet is generally architected in a distributed fashion, certain technical resources have to be regulated at a central point. It is likely that the political discourse on how these resources should be governed will continue.
Internet Identity	The concept of online identity has evolved from simple username/password schemes to much more complex digital representations of our self. Technical communities have been trying to work out how to best express individual and organizational identity on the Internet. Discourse in the area will continue.
Internet Privacy	The amount of our personal data that is exposed on the Internet is dramatically increasing. This includes personal interests, search histories, profiles on social networks and much more. Concerns over the use of and control over such data are likely to intensify.
Digital Divide	Some regions of the world as well as certain parts of society within countries are disadvantaged when it comes to the ability to access ICTs. This applies both to the basic availability of infrastructure and to the knowledge and education to properly use it (“computer literacy”).

Hacktivists	Technically savvy individuals or small groups use the Internet for promoting political and social goals, sometimes near or beyond the borderline of legality.
Artists, Intellectuals	These groups of people are typically concerned with an egalitarian Internet where everybody can express opinions and ideas freely for the purpose of creative interaction, without interference or risk of censorship.
ICANN	The Internet Corporation for Assigned Names and Numbers (ICANN) is tasked with maintaining the elementary infrastructure of the Internet. Its primary objectives are to maintain the network's stability. ICANN is subordinate to the United States Department of Commerce.
W3C, OASIS	The World Wide Web Consortium (W3C) as well as OASIS are the driving organizations behind establishing new technical standards for the Internet to ensure technical interoperability.
IGF	The Internet Governance Forum (IGF) is a United Nations sponsored organization conducting regular meetings to discuss and promote the goals laid out in the 2003 and 2005 World Summit on the Information Society, which are to use ICTs for the benefit of humankind and in accordance with the United Nations Charter.
Energy Concerns	The steadily growing amount of electronic infrastructure required by ICTs consumes more and more energy, the production of which is a potential source of conflicts.
Environmental Concerns	Electronic waste generated by the rapid development of new ICTs continues to cause health and pollution problems, especially when informally processed in developing countries.
Resource Concerns	The requirements for the development of modern ICT hardware include scarce metals and other resources which can lead to human exploitation in regions of their occurrence. One example is the

	essential mineral Coltan, whose mining industry in the Democratic Republic of Congo is known for causing conflicts and massive Human Rights violations.
UNESCO	The United Nations Educational, Scientific and Cultural Organization (UNESCO) has a stake in the future development of ICTs, e.g. through its leading role in the WSIS process and through initiatives such as the *Information for All Programme*, the *International Programme for the Development of Communication*, and the *Charter on the Preservation of the Digital Heritage*.[5]
Cyberwarfare	Cyberwarfare is a relatively young concept which views online computer systems as new kind of battleground on which significant damage can be dealt to an enemy's infrastructure. So far, the potential of cyberwarfare has been mostly speculative, apart from a small number of concrete events such as attacks on the Serbian air defense computer systems in 1998[6], or the Stuxnet virus launched against Iranian nuclear facilities in 2011[7].
Cyberterrorism	Similar to cyberwarfare, terrorists may also be able to attack electronic infrastructure to inflict damage to a state.
Human Rights	A number of organizations (e.g. the Global Network Initiative[8], the Electronic Frontier Foundation[9] or the European Digital Rights Initiative[10]) are committed to protecting Human Rights in the online world, such the rights to access to information, freedom of expression and the protection of privacy.

[5] See (United Nations Educational, Scientific and Cultural Organization, 2003)

[6] See (Arquilla, 2003)

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

[8] See http://www.globalnetworkinitiative.org/

[9] See http://www.eff.org/

[10] See http://www.edri.org/

3. List of Clusters

Based on the above actors and driving forces, clusters will be identified which represent the major possible effects on the future development of ICTs for peace and conflict.

To each cluster, two attributes will be assigned: Their impact on the future (I), and the uncertainty about the way it will actually take place (U). For both attributes, numbers from 1 to 5 will be estimated, with 1 being the lowest and 5 the highest.

(A) Digital Divide	The Digital Divide leads to unequal opportunities, and while there are numerous initiatives to overcome this divide, their successful implementations are questionable. In the future, the elimination or the growth of this phenomenon will have a large impact on peace and conflict worldwide.
	→ Attributes: I=5, U=4
(B) Rise of Cyberwarfare	Cyberwarfare is the most obvious way in which the use of ICTs can influence peace and conflict. Due to the limited experience with actual examples of cyberwarfare, estimations about its actual danger vary.
	→Attributes: I=3, U=4
(C) Securitized vs. Free Internet	From the early days of the mainstream availability of the Internet there have always been utopian visions that this new communication technology would be without borders and free from regulation. Today however, there are voices calling for strong legislation and security on the Internet to counter real or perceived threats.
	→Attributes: I=4, U=5
(D) Centralization vs. Decentralization	Some Internet services are based on a strictly centralized technical architecture, such as the Google search engine or the Facebook social network, whereas others are more decentralized, such as the global e-mail system or the BitTorrent

	filesharing application. Centralized network architectures unify control at a few points in the architecture, whereas decentralized architectures exhibit more democratic and egalitarian characteristics.
	→Attributes: I=5, U=4

Out of the above clusters, two have to be selected in order to build four scenarios. After a closer look, clusters 3 and 4 seem to be interlinked and can be combined into a single cluster, since a highly securitized Internet is also likely to exhibit a strong degree of architectural centralization, while a truly free and open Internet must be based on more decentralized approaches. While the concept of cyberwarfare is interesting and can be incorporated in one or more of the scenarios, it does not appear to have the same kind of world-changing impact that the other clusters have.

Therefore, the selected clusters to produce four scenarios are:

Cluster (A)	Digital Divide Widened vs. Digital Divide Closed
Combined Clusters (C) + (D)	Centralization + Securitized Internet vs. Decentralization + Free Internet

4. Scenario Matrix

The following is the matrix of resulting scenarios based on the selected clusters with high impact on the future and high uncertainty:

	Combined Clusters (C) + (D)	
Cluster (A)	**Centralization + Securitized Internet**	**Decentralization + Free Internet**
Digital Divide Widened	Scenario 1 "Digital Pyongyang"	Scenario 2 "Digital Arusha"
Digital Divide Closed	Scenario 3 "Digital Davos"	Scenario 4 "Digital Porto Alegre"

Based on above scenarios, the following outlines will be assumed in the development of the scenarios' stories:

Scenario 1 "Digital Pyongyang": This Scenario draws a "Big Brother" vision characterized both by highly unequal access opportunities to ICTs and by high securitization, surveillance and regulation. Instead of working as a tool for freedom and democracy, ICTs have become a means to control the masses. The scenario is named after the capital of North Korea, where Internet access is both very limited and highly controlled by the government.

Scenario 2 "Digital Arusha": This Scenario is based on the idea that the Digital Divide widens to such a point where the world's poor regions cannot effectively participate in a global Information Society anymore. A free, decentralized network architecture however enables them to set up their own isolated networks which are mostly incompatible with each other[11]. What follows are processes of localization and nationalism in the online world. The scenario's name is derived from the Arusha Declaration of 1967, in which Tanzanian president Julius Nyerere envisioned a strong national self-confidence.

[11] This idea is sometimes referred to as "Splinternet".

Scenario 3 "Digital Davos": This Scenario assumes the closing of the Digital Divide, giving most people on the planet access to ICTs, however the technical and social network architectures are highly centralized, hierarchical and securitized. As a result, most content and communication flow from a few producers to a large mass of receivers. This system advocates economic opportunities and competition. The scenario is named after the Swiss city Davos, the traditional annual meeting location of the World Economic Forum.

Scenario 4 "Digital Porto Alegre": This Scenario embodies the sum of all utopian visions commonly associated with modern communication technologies. The Digital Divide is closed, meaning that all of humankind has mostly equal access opportunities to ICTs. Also, the technical architectures are highly decentralized and free from regulation, leading to development and intercultural understanding through egalitarian, democratic and creative exchange of ideas. The scenario is named after the Brazil city Porto Alegre, the first meeting location of the World Social Forum.

5. Scenarios

5.1. Scenario 1: Digital Pyongyang

In the wake of the 2000s global financial crisis, governments everywhere in the developed world are severely reducing their financial commitments to development cooperation. As a consequence, NGOs as well as international bodies such as UNDP and UNESCO are forced to more and more narrow down their efforts. While some actors in the international development community argue that the development of ICT infrastructure and the overcoming of the Digital Divide must remain a priority objective despite the reduced financial resources, the majority of organizations shift their efforts to more fundamental human needs. In 2014, UNESCO announces the complete shutdown of the youngest of its four sectors of operation – Communication and Information.

June 23rd 2014

Irina Bokova, Director-General of UNESCO:

"Our budget today is 50% of what it used to be 10 years ago. While we have achieved tremendous successes during the short history of our Communication and Information sector, we must acknowledge that in difficult times like these, books are cheaper than computers, and the world's poorest people need food, water and medicine more than they need the Internet."

In July 2015, an unprecedented event of cyber-terrorism surprises political analysts and security experts world-wide. A large-scale DDoS[12] attack hits the airport of Dubai, United Arab Emirates, rendering all flight control systems non-operational for hours. While emergency systems kick in and prevent worse, one approaching Airbus A380 plane crash-lands in the Persian Gulf, killing 64 passengers. The source of the attack is discovered to be a large network of OLPC laptops[13] in the developing world, which are found to have been exploited and remotely controlled by an unknown group of hackers. This has been made possible due to a so far unknown, serious software vulnerability in the laptops' operating system. The exact source and motivation for the attack is never discovered, however, in the face of the large number of already deployed OLPC laptops around the world, the only feasible technical solution is to severely reduce the laptops' Internet connectivity, up to a point where using them even for sending a simple e-mail becomes a time consuming task. In the wake of these difficulties, many projects to develop new ICT infrastructure are canceled, further widening the Digital Divide.

Realizing the increasing risks in an interconnected world, securitization debates about governmental control over ICTs intensify. After many years of political and legal

[12] A Distributed Denial-of-Service (DDoS) attack confronts an electronic system with a large number of malicious requests, to the point where legitimate operations can no longer be completed.

[13] The One Laptop Per Child (OLPC) initiative aims to provide each child with a rugged, low-cost, low-power, connected laptop. These laptops have the ability to connect to each other easily, forming a so-called ad-hoc "mesh" network. See http://one.laptop.org/

discussions, on February 1st 2016, the Czech Republic as the last member state of the European Union finally implements EU Directive 2006/24/EC (the "Data Retention Directive")[14]. From now on, state authorities in the entire EU store all data about access and usage of electronic communication services, e.g. phone numbers, text messages, e-mails, IP addresses, etc.

February 1st 2016

José Manuel Barroso, President of the European Commission:

"The Internet is not a technology that is beyond the rule of law, as some may think. We have seen that insufficient control can directly result in the loss of life, and we do not want to see another Dubai happen in the heart of Europe. We cannot accept a space in which criminal acts can freely take place outside of the union's executive reach."

In the following years, the EU Directive 2006/24/EC is continuously amended to further expand control and surveillance possibilities, leading to the creation of a "virtual Schengen border" that puts strong oversight and constraints on all electronic communication within Europe. Citing security concerns, many other governments world-wide invest heavily in measures to increase their monitoring and surveillance abilities of telephony and the Internet. The People's Republic of China with its long experience in operating national firewall systems becomes the world's leading provider of costly but effective Internet security and censorship technologies. As a result, high-speed Internet technologies become much more expensive for end consumers. This development further widens the Digital Divide and turns Internet access into a luxury commodity even in developed nations.

In late 2019, ICANN receives a United Nations mandate to greatly expand its scope to also act as a centralized security oversight agency, uniting existing national efforts into a single global system. From now on, ICANN is not only the governing organization of basic technical resources such as IP addresses and domain names, but also the issuer of

[14] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

a new world-wide ID system that becomes mandatory for all Internet users. All access to the Internet and all communication can now be monitored and directly traced back to an individual's identity, eliminating all anonymity. There are both winners and losers in this highly securitized Internet. On one hand, phenomena of cyber-crime such as identity theft, spam or the distribution of child pornography have been completely eliminated. Individual citizens can file requests to ICANN to request websites to be removed from the Internet if they damage their reputation. On the other hand, cases of denunciation are on the rise where innocent people are incorrectly accused of cyber-crimes, and the sense of freedom and openness that was typical in the early days of the Internet has vanished.

In 2020 in Bangalore (the "Silicon Valley of India"), a student movement simply calling itself 01101001! is formed to oppose the highly securitized and unequally distributed ICT services. The movement's motto is

"This is not the Internet as it should have been!"

The 01101001! movement attempts to unite efforts around the world to engage in nonviolent struggle against what it describes as a global digital dictatorship. Activities include the development of alternative and anti-censorship networking technologies, as well as street action in many capital cities in the world. However, given ICANN's totalitarian control over all Internet identity and communication, 01101001! fails to reach a large audience with their political messages, and is eventually declared a terrorist organization by most of the world's governments.

5.2. Scenario 2: Digital Arusha

In the early years of the 2010s, efforts to overcome the Digital Divide are only moderately successful. Projects such as the OLPC initiative or UNESCO's *Information For All Programme* (IFAP) improve connectivity to some extent in developing nations. At the same time however, the technological advances in the developed world do not simply stop and wait for others to catch up. On the contrary, universities as well as young Silicon Valley startups continue to increase the pace at which new technologies are developed. These technologies offer more and more possibilities for Internet users, for example as live, personal video broadcasting to a large audience, or high-resolution 3D photographs on web pages. However, these new innovations consume more and more bandwidth, which is available only in privileged parts of the world. While in 2011 the average size of a single Facebook page was around 200 kilobytes, by 2013 this has grown to 4.5 megabytes. As a consequence, while Facebook is in principle a popular service all around the world, it becomes less and less usable in practice in the underdeveloped nations of Africa, Asia and Latin America. Despite the expanding ICT infrastructure in those regions, the Digital Divide is therefore still effectively becoming wider. Western political and economic leaders pay little attention to this fact.

In October 2014, frustrated by the continuing unequal opportunities, the African Union holds a conference called "A Digital Future for Africa" in Arusha, Tanzania, where high-level delegates of the member states discuss strategies for the further development of the continent's Information Society. The conference ends with a sensation: The unanimously adopted outcome resolution calls for an independent Internet to be established on the African Continent, using existing hardware infrastructure such as cables, servers and routers, but being logically separated from the global network. The resolution is filled with a strong spirit of self-determination and self-confidence.

October 28th 2014

Vincent Karega, Minister of Infrastructure of Rwanda

"Perhaps it is a historic coincidence that here in Arusha, Julius Nyerere in 1967 called for economic self-reliance for Tanzania. Today, we are calling for information self-reliance for all of Africa. We can no longer count on

Western charity to build our ICT infrastructure, we must do it ourselves. After all, who other than Africans can possibly understand African information and communication needs?"

ICANN issues repeated warnings against uncoordinated efforts to build isolated network structures, but the organization is technically powerless to prevent such steps. On January 1st 2015, the African Internet becomes effectively separated from other continents. Independent DNS root servers that control the Internet's domain names are set up in Cairo, Kinshasa, Nairobi and Johannesburg. In practice, this means that African users can no longer type addresses such as www.google.com on their computers, and e-mails can only be exchanged within Africa itself. While initially there is considerable public resistance against this drastic step, African entrepreneurs quickly embrace the newly found self-confidence and sense the opportunity to build websites and services specifically for African traditional needs and culture. To the surprise of the rest of the world, the separated African Internet flourishes, and by 2018, African users become the most computer-literate people in the world, having built their own Internet according to their own needs. Economic advantages follow quickly in the form of rising GDPs and less political dependency from the Western world and China.

Impressed by this unique success, regional organizations in other continents decide to adopt the same strategy. Within only one year, by the end of 2019, Latin America, Asia, Australia and even Europe follow Africa's lead by also designing their own isolated Internets. All of the separate Internet regions develop a wealth of new social networking services. Each one of them differs from the others, reflecting cultural peculiarities of the respective cultural regions. For example, while the leading social network provider in North America – Facebook – is built on the principles of individual identity, personal profiles and friend connections, the leading African social network service – Kiboko – emphasizes support for traditional African forms of social organization such as tribes and polygamy.

While some consider this fragmentation of the Internet to be contrary to its early vision of interconnecting the whole world, others – such as UNESCO – consider it a fruitful way to avoid cultural imperialism and to preserve the heritage of traditional ways of life.

January 20th 2020

Sir Tim Berners-Lee, inventor of the World Wide Web

"The original idea of the web was to unite all content and communication in a single network and addressing space. Today's paradigm of fragmentizing the Internet is not consistent with this vision. But, you know, if this is what makes people happy and serves their needs, then maybe it's not such a bad idea after all!"

While different parts of the Internet are logically isolated, with each zone developing its own services and communication patterns, the physical connections between the individual zones continue to exist. Studies report that 90-95% of Internet users world-wide are satisfied with accessing only information within their own zone, however, special software is available to also connect to other zones if desired.

June 30th 2020

Mozilla Firefox version 7.6.17 is released. The popular web browser software now has built-in functionality for selecting one of the six major Internet zones.

5.3. Scenario 3: Digital Davos

In 2011, the World Economic Forum releases a report titled "The Emergence of a New Asset Class". In this report, it is argued that

> *"Personal data will be the new oil – a valuable resource of the 21st century. It will emerge as a new asset class touching all aspects of society."*

In the following years, the amount of data that is being collected, stored and used online explodes. A wealth of new standards and technologies is being developed by the W3C and OASIS to make the exchange of personal data between individuals and organizations simple. The vision of the Semantic Web[15] becomes reality by making all data online machine-readable, interoperable and interconnected. Every single bit of personal information has an immediate monetary value, and a marketplace of buyers and sellers emerges. In this digital economic system that comes to be known as Web 3.0, personal data becomes the new currency.

This boom of the new personal data market interestingly boosts measures to overcome the global Digital Divide. The more people are able to access the Internet and other electronic communication services, the bigger the amount and the value of usable data becomes. Therefore, the objective of connecting more and more people world-wide to ICT infrastructures shifts from an ethical goal to an economic incentive. In the following years, technical universities and Internet startup companies achieve what nation-states and international organizations have failed to do: The development and actual deployment of low-cost but effective networking infrastructure and computer hardware throughout the developing world. In 2013, 80% of the world's population has access to the Internet, with the percentage continuously rising.

As companies in Silicon Valley engage in fierce competition for users and their personal data, a strong centralization process sets in. By 2014, Facebook – controlling the online identities and personal profiles of over 3 billion people – has won the race as the leading provider in the personal data market. New functions enable Facebook users to make money by selling their profile data to marketing and advertising companies. The estimated value of Facebook – which by now is a publicly traded company – has

[15] The Semantic Web's basic idea is that the World Wide Web consists not just of a web of human-readable documents, but also of machine-readable data.

multiplied by the factor 5 since the year 2000. Warnings by human rights activists and data protection advocacy groups against this centralization of power are ignored by the general public.

November 21st 2014

Excerpts from a TV discussion round about the personal data economy

Rico O., Director of the Personal Data Initiative, World Economic Forum:

> *"The ecosystem around personal data has created a wealth of new economic opportunities. It has lifted us out of the financial crisis, it has brought people in the developing world online, and it benefits us all in everyday life. Any hard-working individual with an entrepreneurial spirit can participate in this system and launch a successful business."*

Maria B., Internet User:

> *"I think it's fantastic. Not only can I make money online by selling my data, I also get new useful services from it. I downloaded an app for my iPhone 7 that collects all data about my driving habits while I sit in my car. Now, my computer can automatically find the car insurance that suits me best."*

Prof. Edward M., Columbia Law School:

> *"Facebook has obtained more personal data about people than all authoritarian regimes in history combined have ever managed to collect about their citizens. This is highly dangerous, and we will soon have to pay the price."*

Facebook, Twitter and Youtube also continue to expand their reputation as being tools for overcoming dictatorships, and for supporting democratization processes all around the world. In late 2015, the separatist Uyghur Dragons – a Facebook group with over 3 million members – challenges the People's Republic of China's government by declaring independence of the Uyghur nation via a Twitter message. The movement receives strong international support from Western governments as well as from millions of Internet users. While China barely manages to prevent complete secession, it is forced to grant large autonomy rights to the Uyghur people. Inspired by this success, the Lakota Republic movement in the United States launches a similar campaign, demanding their own independent nation within the borders of the 1851 Treaty of Fort Laramie, which would cover about 200,000 km^2 in the middle of the United States. The movement however is stopped in its early stages, after the social network accounts of its leaders are

terminated by Facebook without warning, citing violations of its Terms of Service. Rumors that Facebook has been pressured to this measure by the United States government are never confirmed. Political observers in Europe estimate Facebook, Twitter & Co to be a stronger weapon of political hegemony than nuclear deterrence.

January 20th 2017

After having reached the end of his second term in office, former president Barack Obama joins the Facebook board of directors and issues a joint press release with CEO Mark Zuckerberg:

"We are both American patriots. Today, Facebook is our primary diplomatic instrument for bringing peace, justice and democracy to the world, and we will continue to strengthen this instrument."

In 2018, The Economist publishes a study saying that young adults who are not on Facebook have a 50% smaller chance to obtain a college education. In addition, people who do not sell their data online are found to be at an increased risk of poverty. The study concludes that there is a direct correlation between the level of participation in the personal data economy, and one's financial, educational and social status. In the same year, UNESCO releases a report titled "The State of the World's Cultural Diversity". The report says that over 200 languages have become extinct in the last 5 years, and that thousands more are at risk. As a cause for this development, the report mentions the increasingly connected, hierarchical and homogeneous Internet, in which there is a small core of actors controlling most of the web's content and data, and a large periphery of users who in practice have little choice but to participate. The UNESCO report coins the term "data imperialism".

In 2020, the entire world is connected. However, the distribution of control over content and data has become highly unequal. On September 11th 2020, a previously unknown terrorist organization calling themselves the Digitaliban successfully conducts a cyber-attack on Facebook's main data center, deleting millions of user profiles from its database. While most of the data can be restored from backups within a week, a few

thousand user accounts remain permanently lost. Security analysts, policy makers and Internet users world-wide sense the dawning of a new era, as the following statement appears on Facebook's front page for several hours:

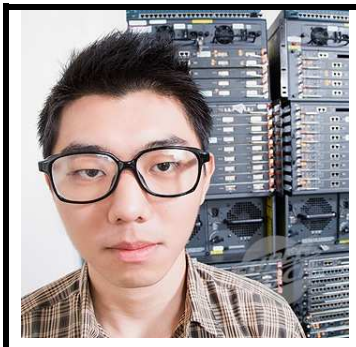
"In the Name of Allah, the Most Gracious, the Most Merciful. We are fighting because we have been attacked first. This time, our native lands are occupied by Western crusaders not through military power, but by limitless control over our information and communication. In doing so, you humiliate us and steal our digital wealth. We are the Digitaliban, and it is our sacred duty to fight against this oppression using the same weapons that you are using against us."

5.4. Scenario 4: Digital Porto Alegre

At the beginning of the second decade of the third millennium, the world continues to become more interconnected, further reducing barriers of both space and time. With globalization also comes an increase of public awareness about global challenges. Global warming, transnational terrorism, mass migration and global financial problems are all on one hand quickly brought to people's attention through ICTs, but on the other hand also partially caused by those very technologies. With individual nation-states, economies and even international organizations proving unable to deal with such challenges of a global scale, it is an emerging global civil society that instead develops a historically unique global sense of responsibility to save the world from irreversible damage. Individuals, NGOs, trade unions, faith-based groups and independent media all form new global networks characterized by shared values and combined action.

In January 2013, an informal global solidarity movement founded by a group of students from the Polish Politechnika Warszawska[16] makes a pledge to overcome the Digital Divide within two years. This movement calls itself "Digital Solidarność" in allusion to the historic Polish trade union. What is initially dismissed as impossible by spokespersons of national governments and international organizations is indeed achieved by this shining example of global civil society action. Through a well-organized combined effort of world-wide fundraising, hardware recycling and the invention of new networking devices and software, most of the developing world is provided with high-speed Internet access by the end of 2015. One key invention in this process is a new wireless network standard, designated IEEE 802.11y, which operates in the 1.2 GHz frequency band and makes it possible to connect entire cities and rural regions with only a few antenna stations.

[16] See http://www.pw.edu.pl/



October 25th 2015

Kimo Takagi, chairman of the Japanese chapter of Digital Solidarność

"Providing modern Internet access throughout the developing world has never been a matter of financial or technical obstacles. What was missing was only the political will. Our members are now accomplishing what governments have failed to do: Fulfill basic human rights in the Information Society. Because we are all one, and in the end we all are what we are only because of what we do for others."

Photograph of an IEEE 802.11y antenna station deployed in the Cunene province in Southern Angola. At a cost of only USD 20,000, the system can deliver high-speed wireless Internet connectivity to an area of 50,000 km^2.

Acknowledging the surprising success of Digital Solidarność, the dominant Internet services such as Google, Facebook, Twitter and Youtube hastily expand their server resources in order to prepare for an expected increase in users wishing to sign up for their services. However, instead of stopping at its stated goal of bringing Internet connectivity to the world, Digital Solidarność continues to also develop software that promotes a more democratic and egalitarian world. In 2016, its flagship project is now called Sieć, which is a social network and messaging platform similar to Facebook and Twitter, but built on a decentralized peer-to-peer technical architecture which resembles the global e-mail system. On Sieć (Polish for "network") there is no single authority, anyone can integrate new servers and applications with the network, personal identities are completely anonymized, and all data and communication are protected by cryptographic methods.

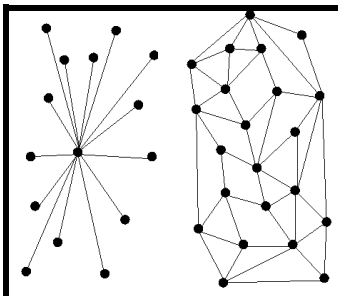


Diagram comparing a centralized social network such as Facebook (on the left) with a decentralized approach such as Sieć (on the right). The decentralized structure is much more resistant against disruption and censorship, and makes it easy to efficiently pass messages as well as add/remove connections at any time. It has no single point of control and encourages heterogeneous relationships.

This network becomes highly successful up to a point where millions of existing users abandon Facebook and Twitter, and join Sieć instead. Search engines such as Google also dramatically lose in importance and value, as they turn out to be unable to apply their search functionality to the decentralized and encrypted network. Over time, Sieć evolves into much more than just an alternative to Facebook and Twitter, it becomes the basis for a conscious global civil society that begins to address more and more global problems from illiteracy to poverty. Furthermore, it encourages intercultural dialogue between the world's many cultures, eliminating the root causes of many ethnic conflicts. The World Social Forum with its motto "Another world is possible" greatly supports this development, concluding at its 2018 summit that

> *"This is the technology we have been waiting for. It liberates the oppressed from political hegemony, economic slavery and propaganda at the hands of the ones in power. It is the catalyst for removing social inequalities and structural violence. What we are witnessing is both the voice and the instrument of a historic process of emancipation."*

Other actors however voice concerns about the rise of decentralized Internet services.

February 8th 2019

Ronald Noble, Secretary General of Interpol

"While we acknowledge and generally welcome the freedom and global nature of Internet services such as Sieć, we have to be aware of the fact that they also provide freedom for criminals. At the moment we do not have the means to effectively

prosecute criminal acts on the Internet, such as the distribution of illegal material or the organization of terrorist attacks."

As of 2020, all attempts by governmental authorities and well-funded corporations to impose stronger levels of control on the Internet are easily countered and circumvented by technologists of the Digital Solidarność movement.

6. Conclusions

The presented scenarios illustrate four potential future evolutionary paths of ICTs and their consequences for peace and conflict in the world. All the scenarios have positive and negative aspects embodied in them. It should be pointed out once again that the purpose of this exercise is creative thinking and the stimulation of ideas, rather than accurate prediction. Therefore, none of the presented scenarios is itself very likely to actually come true. What is almost certain however is that at least some aspects and ideas from the presented developments will be observed in the future. For example, it is likely that Facebook will expand its role as a predominant identity provider on the Internet (see Scenario 3 "Digital Davos"), and that at the same time efforts to protect data will grow (see Scenario 1 "Digital Pyongyang"). It is also likely that countries in the so-called developing world will increasingly develop their own content and services (see Scenario 2 "Digital Arusha"), and that ICTs will be used for idealistic purposes by an emerging global civil society (see Scenario 3 "Digital Porto Algre").

On a personal note, I find Scenario 4 "Porto Alegre" the most desirable one, for its user-centric, egalitarian and human rights based approach. I believe that this scenario is the one that Internet visionaries, entrepreneurs and engineers alike should be working toward.

7. Bibliography

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

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

Mann, S. (2011, 2 19). *Twitter diplomacy emerges as new tool in US arsenal.* Retrieved from The Age: http://www.theage.com.au/world/twitter-diplomacy-emerges-as-new-tool-in-us-arsenal-20110218-1azov.html

United Nations Educational, Scientific and Cultural Organization. (2003, October 15). *Charter on the Preservation of Digital Heritage.* Retrieved from http://portal.unesco.org/en/ev.php-URL_ID=17721&URL_DO=DO_TOPIC&URL_SECTION=201.html