5

FROM A HORSE TO HUAWEI AND FROM TROY TO TWITTER: HOW TO REBUILD TRUST?

Christoph Stückelberger

The escalation of US-China conflicts translated into harsh unilateral measures of the US against Huawei, Tiktok and Wechat.[1] At the same time, the US congress mistrusts the monopoly structure of the US giants like Google, Facebook and Amazon and plans additional antitrust legislations. This current situation fuels a cycle of mistrust amongst governments, companies and citizens. This article places individual companies in the broader geopolitical, geo-economic and ethical context and proposes four steps to rebuild trust in order to serve humanity by prosperity, harmony and peace. This is more needed than ever in the current shaky world of the Covid pandemic, Ukraine war, still increasing polarization between Superpowers and the global technological race.

---

[1] Prof. Dr Dr h.c. Christoph Stückelberger, Professor of Ethics (emeritus in Basel), Visiting Prof in China, Russia, UK, Nigeria. Founder and President of Globethics.net and other not-for-profit global foundations.

5.1 The Trojan horse

The hot conflicts around the tech giants such as Huawei and Tiktok, a product of ByteDance, but also the antitrust report of the US Congress in October 2020 on Amazon, Apple, Facebook and Google are in its essence 3200 years old. In the Trojan War (1260-1180 BC), the Greek aggressors built a huge wooden horse with elite soldiers in it and conquered the independent city of Troy (now in Turkey, close to Greece and Istanbul). The ancient superpower Greece used advanced technology, cunning and deceit to entangle and dominate a small independent city-state.

Today, the place of war is not primarily physical, but virtual in the digital world. The digital economic war is predominant, but digital military wars are already partly happening. The Trojan Horse is even used as term for malware installed in software and the backdoor of the wooden Trojan Horse is the backdoor on computers and IT systems installed by secret services, hackers and all the other virtual 'soldiers' and 'armies'. A backdoor is a covered method to bypass a normal login on an electronic device and thus getting illicit access to protected data. A backdoor can either exist with hardware or software, which allows for intrusive data access or influence in a digital system. More often a software backdoor can also be installed by a Trojan Horse. There is a thin line between legal and illegal as the producer may also use backdoors to repair a system.

Therefore, nothing new under the sun? Indeed, in ethical perspective, the old type of power concentration, aggression, cunning and mistrust seems to be repeated throughout human history. The difference lies in the modern sophisticated technological software, in the global dimension of the cyberspace and therefore of the conflict, and in international cyber-related communication means which makes secret actions more and more challenging.

5.2 Mistrust: Huawei and Tiktok as scapegoats

The conflict with Huawei and Tiktok was mainly provoked by the American President Trump's attack that the two companies provide a backdoor to the Chinese government and thus provide user data. Similar accusation was against Wechat, the Chinese giant for mass communication like Whatsapp in the "Western" world. This was given as a main reason to ban or control these companies in the US and in its fairway in other countries like India, Pakistan and others. On the other hand, Huawei signed "no backdoor agreements" and cooperates with six external verification centers providing technical verification and evaluation platforms (Cyber Security Centers in Banburry/UK, Toronto/Canada, Bonn/Germany, Dubai/Emirates, Dongguan/China and Brussels/EU). Huawei holds 16243 patents with IP protection, of which 11,096 outside China. "Huawei operates independently from government", is Huawei's self-declaration.[2] The founder and CEO Ren owns only 1.04% of the shares and 98.96 are in the hands of the employees. Huawei called in the Covid and security challenges for global cooperation by developing trustworthiness standards, innovation and refining infrastructure policies.

In response to the unproven accusation of Huawei allowing the Chinese governments using a backdoor to the data, Huawei launched a proactive "zero trust" approach. The invite the customers not to trust Huawei, but to critically examine themselves the software and hardware back to the source code and then get certainty that no backdoor is used by own examination. For this objective, Huawei established several test centers for potential and existing business customers. The largest is the Cyber Security Transparency Center in Brussels. The center was analysed

[2] *Who Are We, Huawei?* Huawei Corporate Presentation, internal, slide 24.

among others by an independent Swiss journalist who described the experience of the visit in an article.[3]

Ironically, the US work with accusations against Huawei of backdoors in software without delivery of proof whilst using same methods of backdoors themselves. The US National Security Agency (NSA) admitted already in 2015 that they use backdoors as built-in access to companies' data. Chinese could not prove that they have no backdoors and that they stopped industry espionage. Under such circumstance, the question is: who bears the burden of proof - the accuser or the accused? The fact is: Huawei openly announced in Brussels that it is willing to accept a system of supervision by European governments, customers and partners. The ownership structure of Huawei shows that even though officially the majority owners are the employees, de facto the union. It boils down that Huawei's sin is its corporate nationality with its headquarter in Shenzhen, China. The conflict is a form of US sanction against China. However, sanctions mainly provoke a push for more diversification and homemade production (Iran and Russia) but at the end often strengthen the sanctioned country and leads to the opposite outcome intended. China has means for retribution. US depends much on pharmaceuticals and hardware from China. As Huawei delivers components of tech on 5G to 170 countries,

[3] Christoph Hugenschmidt, *Wie Huawei Cybersecurity praktiziert und wie transparent das wirklich ist – ein Besuch im Cyber Security Transparency Center in Brüssel*, in Marc Furrer (Ed.), *Selbstbestimmt. Sind souverände Kommunikationsnetze in der Schweiz möglich?*, Berne, Stämpfli Verlag, 2022, 89-95. (Translation of the article title: How Huawei practices cybersecurity and how transparent it really is – a visit in the Cyber Security trasnsparency Center in Brussels).

the whole world is adversely affected. Due to the US ban of Huawei technology, many companies must decide if they should still use Huawei and risk US sanctions or work with China or both.[4]

The US actions against Tiktok are somehow different and somehow similar to the Huawei case. At the core of the conflict is a pure and brutal power game about dominance in the global market of IT services (Huawei) and the potential influence on masses of consumers and thus large parts of a population (Tiktok). Conquering a country or a city does not need conventional arms, occupation and solders, but technology, software control, big data access, artificial intelligence – and people who use all these electronic devices on a daily and many on an hourly basis.

Twitter was originally a short message service for citizens and consumers. With President Trump using it as daily channel for top level political as well as personal messages, it became strongly politicized up to the level, that Twitter had to introduce voluntary control mechanisms of content in order to regain some credibility and trust. The same time, more and more politicians use this fast-communicating channel for official, even governmental messages.

Huawei, Tiktok and Twitter became somehow scapegoats in the geopolitical power game between US and China. The larger historical context is the continued shift of geopolitical power from US to Asia. Whereas the 19th century was seen as the century of Europe with the large colonial powers Great Britain, France, Spain and Portugal, the 20th century was the century of America (even though during Cold War in competition with Russia). But with the rise of South East Asia, its tigers, and especially the fast economic (and less political) rise of China, the 21st century is seen as

[4] Under pressure of the USA, the leadership of the famous Swiss Federal Institute of Technology ETH has forbidden to all staff and researchers to use Huawei technology, which created strong reactions on academic freedom. *5G: USA warnen nachdrücklich vor Huawei*, Sonntagszeitung 2 Feb 2020, 9.

century of Asia. Many analyses of political scientists and economists confirm this. Technologies play – as always in human history – an instrumental role in this shift of power. Huawei and Tiktok are just two symbols for it. Technological struggles about backdoors, data control, national sovereignty and values-related issues of human rights or freedom versus control and discipline are mainly arguments to justify market interventions via technological and political restrictions, but the core of the struggle is a pure brutal power struggle for dominance.[5]

During the Cold war 1945-1989, the military-industrial complex was the symbol for the collusion between military power and industrial technical dominance. The current conflicts in the new beginning (and hopefully soon ending) Cold war is the same, with the difference, that it is no more the heavy industry, but the IT industry which is the sensitive sector. The result is the same: deep mutual mistrust of the superpowers US and China. Europe as Africa and South America are in between and risk to loose continental unity as many countries are forced to decide if they belong more to the Asian or to the North American bloc. The North American neighborhood does appear more concerted in action at the taming of the US.

5.3 Antitrust: GAFA and BATH as 2x4 superpowers

Another reality, which creates increased mistrust between powers and continents is the huge economic power and outreach of a few mega-companies, mainly from the US Silicon Valley: Google, Apple, Facebook and Amazon, also called GAFA. Their counterparts in China are Baidu, Alibaba, Tencent called BAT, but I add Huawei which we then call

[5] Stückelberger, Christoph, *Globalance. Ethics Handbook for a Balanced World Post-Covid*, Geneva: Globethics.net, Aug 2020. Chapter 7.3 on Cyber-World, 243-257. Revised and enlarged edition *Globalance Towards a New World Order. Ethics Matters and Motivates*, Geneva: Globethics.net, Nov 2022. Free download www.globethics.net/globalance.

BATH. In the last century, the Multinational Companies (MNC's), which have been economically more powerful than countries, covered the oil, gas, mining, food and few other sectors. Some of them are still very powerful, but the focus turned in the 21st century to those few extremely large companies dealing with Big Data. They are champions in search machines (Google, Baidu), databased global online shopping platforms (Amazon, Alibaba), social media platforms (Facebook, Tencent), mobile phones and their applications (Apple, Huawei) and more and more a combination of them, linked with online payment systems and cloud services. These are eight mega-players. National and continental regulators such as US and EU now strengthen their efforts to guarantee at least some free and fair market mechanisms. The Anti-Trust Report of the US Congress of October 2020[6] looks at the competition in digital markets which may lead to a restructuring of the GAFA companies in order to reduce their oligarchy.

This concentration of economic and technological power is not only a danger for a social market economy, but it is also seen as a mounting threat for democracy. The potential or real influence on the political systems becomes very large, as the suspicion or reality of influencing elections by these super-companies pops now up in almost all elections around the globe. Since the election campaign and presidency of Donald Trump, Tweet became an official means of direct communication of politicians circumventing many kinds of traditional diplomatic ways of political communication.

In addition, behind this struggle is the fight for access to and control of semiconductors. Semiconductors as cutting-edge technology, key for all these digital mega-players. Data analysis, robotics, AI, surveillance technologies, 5G networks, satellites, computing and storage capacities all need high performing semiconductors. These chips are the central

---

[6] I*nvestigation of Competition in Digital Markets*. Majority Staff Report and Recommendations. Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, United States, 6 Oct 2020.

nerve system of modern technologies. There are only three top semiconductor producers left from over 20 producers few years back: TSMC in Taiwan, Samsung electronics in South Korea and Intel in the US. 50% of all semiconductor chip sales are done by US-companies, but worldwide 70% of these chips are produced in Taiwan![7]

5.4 Satellites, clouds, blockchain, darknet, secret services

An additional dimension in the global techno-economic-geopolitical war is the access to and control of satellites. The SpaceX Company of Elon Musk only, with its Starlink[8] programme already placed 775 satellites by 6 Oct 2020 and got the approval by the US Federal Communications Commission (FCC) to place 12'000 satellites in the airspace and submitted respective filing to the International Telecommunication Union ITU in Geneva. Additional 30'000 satellites are planned. Starlink is a private company, but the US Air Force already tested Starlink satellites in 2019 and 2020 for its support of Battlefield Management Systems for air and terrestrial exercises. Again, this increased mistrust over dual-use (civil and military) digital technologies where satellites will be much more important than cables in the sea, invokes high political and diplomatic sensitivity. The permission and control over the backdoors of these satellites - by far the largest in number in the space, owned by a private US company, already used by US Air Force, and in future broadly rented to countries and customers around the globe - is vital to national security and corporate profitability. Competing satellite constellations have been announced by Samsung, Amazon and some small companies, but all of

[7] Gisiger, Christoph, *Chips erobern die Welt*, Themarket.ch, 2 Oct 2020, 8-9.

[8] Latest info from https://en.wikipedia.org/wiki/Starlink, revised even on the day when I wrote this article: 11 Oct 2020. See revision history https://en.wikipedia.org/w/index.php?title=Starlink&action=history .

them are much smaller than Starlink and may even not be launched. Starlink is by far the most advanced. China is active in space technology for Moon and Mars, but much less with communication satellites stationed around the globe like Starlink.

Already estimated 40 percent of all internet information exchange and trade is conducted on the Darknet, established originally by the US secret service as an invisible parallel internet in the dark. It is now the playing ground for thieves and hackers, arms traders and secret services and all who want to be invisible in the internet. I guess that not only all armies and secret services in the world, but also all GAFA and BATH companies have their respective accounts on the dark net. A global company cannot analyse the global market by knowing only 60 percent of the visible market and not knowing the 40 percent of the invisible market. The Darknet is ethically not acceptable as it legitimizes a double morality and double world, the visible and invisible. Therefore my radical suggestion to try to destroy the Darknet with all necessary legal and economic means. But an international Cyber-law conference in Delhi in November 2019, most panelists from cybersecurity expertise to companies to politics expressed some reasons to justify the Darknet as useful for secret services, even as protection for exposed human rights defenders to spread their information.

5.5 How to rebuild trust?

The aspects mentioned until now seem to cover very different sectors of industry and technology. The goal here is to show that they are interdependent: entrepreneurial competition between two times four (2x4) giants US-China, then the race for technological dominance and access to key technologies such as the chips, and all this linked to geopolitics with – mainly unexpressed – military and cyberspace interests.

There is not a conspiracy behind, but there is interconnectivity. For those who do not understand the complexity and the interconnectivity –

and most of the world population including myself – re-act with uncertainty or mistrust against one or the other company or government. The debate about a single company like Huawei or a government like the US or Chinese leaders is an expression of it.

However, the reality is that the complex global technological interdependency leads to geopolitical power games in order to reduce complexity and dependency and to increase sovereignty and tech-no-political dominance. Populism is a dangerous expression of this attempt to reduce complexity.

What is then the way to reduce mistrust, to rebuild trust? We need to find the right balance[9] between sovereignty and dependency, and ways of fair international cooperation, without driving to war and military 'solutions' of the problem. Confrontational or winner-takes-all approach would only increase uncertainty, vulnerability, and produce manifold costs, economically, politically, ethically and last but not least of human lives. Let me propose for actions to rebuild trust:

5.5.1 Building trust by multilateral technological controls and standards

Self-declarations by companies and governments on the issue transparency and accountability are not worth the paper it is written on, regardless their solemn pledge that they only want the best for humanity and do not use software companies for their military or political interests. Self-declarations – even if they are honest as some are – cannot create trust. That is the simple reason why certifications and standards set by third parties are needed and practiced in all sectors, and along the entire value chain - from technical process to output quality. This is also noticeable from education standards to publications quality, from vocational training

[9] Stückelberger, Christoph, *Globalance. Ethics Handbook for a Balanced World Post-Covid*, Geneva: Globethics.net, Aug 2020. Chapter 7.3 on Cyber-World, 243-257. Free download www.globethics.net/globalance.

to admission of religious organisations by states, from energy standards to disarmament control.[10]

Huge progress was made in the last hundred years in all these fields of technological control and international standard settings. From private standards like ISO or fair trade labels to governmental and global multilateral institutions like ILO in labor standards, ITU in telecommunication standards, WIPO in intellectual property standards, Unesco in education standards, IATA in airlines standards, IAEA in atomic energy standards, UNEP in environmental standards, the conference for disarmament for control of signed disarmament conventions. Many of these organisations are based in Geneva/Switzerland, just 1-2 kilometers from my office in Geneva. Geneva therefore is called the international city for standardization.

Each generation has to set standards and controls for new sectors and technologies. Cyber-technologies are certainly a main technological driver. They develop extremely fast, linked to Artificial intelligence, mass communication, big data use etc. It is not by chance that the 2x4 super-power-companies GAFA and BATH, mentioned above, are all somehow based on and driven by cyber-technologies. It is therefore 'logical', that they are now in the eye of the storm. Huawei has to be seen not as a single case, but as part of this larger geopolitical context.

Rebuilding trust in these GAFA and BATH giants needs more than a one-by-one critique. It needs an international standard and control system. The international Atomic Energy Agency (IAEA) in Vienna was founded in 1957, when nations feared that peaceful atomic energy production could be used for atomic weapons. Mistrust was answered by a global control mechanism. Even though we know its limitations, it was a key step forward for peaceful use of atomic energy. The same is needed today

[10] More in Stückelberger, Christoph, *Global Trade Ethics*, Geneva: WCC, 2002, 71-102.

for a controlled and trustworthy use of cyber-technologies. The International Telecommunication Union (ITU) is already partly linked to it, but its mandate is not broad enough to deal with these security-related mistrust of the GAFA and the BATH companies. Their self-policing is a good beginning, but far from enough. The telecommunication companies themselves have a very strong say in ITU, which is on one hand good in terms of the multi-stakeholder commitment, but also hinders binding controls in sensitive issues of dual use for military and civil telecommunication.

I suggest an international effort with the UN and other multilateral actors to create a multilateral, binding system for cyber-technology control. It could, e.g., be called ICTA: International Cyber Technologies Agency, similar to IAEA. There are of course numerous good cyber security companies and international associations, but they are mostly private and therefore cannot fully rebuild the trust mentioned here, as they do not have the multilateral character of intergovernmental efforts.

Most multilateral dialogues and proposals surrounding the digital industry focus on facilitation of cross-border data exchange in economic terms. The dimension of measures to prevent unfair data exploitation is side stepped. On top of international standard, this digital world also requires a globally empowered arbitration apparatus to adjudicate on the ground of fairness and justice, which can largely diffuse retaliation and confrontation at the unilateral will and interest of one party involved in a disputable situation. Global trade surged in a more orderly fashion after the World Trade Organization (WTO) is vested with the dispute settlement mechanism with few instances of trade disputes escalating into a hot war.

The European Union, France, Germany, China, Russia, African Union and others are still promoters of multilateralism. They have different interests and with the current resistance of the USA against multilateralism, it is heavy to make progress. Nevertheless: where there is a will, there is a way.

5.5.2 Building trust by shared values and virtues

Building trust on the basis of shared values and virtues is a necessary approach in addition to building controlling institutions. It is even a precondition to control, since companies and countries are only willing to cooperate in a multilateral setting when there is a minimum of common goals, or at least a balance of interests, be it negative (reducing fear of the other's cyber-attacks, spying and own vulnerability), be it positive (more own security, reduced security costs, fairer competition, lower risk of war etc.).

The modern phase of globalization since 1990 showed the need for universally shared values. The Global Ethic Declaration of Hans Küng with the Parliament of World Religions agreed on a minimum of five values. My own works on a global balance of relational values (above footnote 7) show that it is possible to reach common values. The UN Sustainable Development Goals (SDGs) and UN Global Compact are globally agreed set of goals, based on common values. This shows the existentiality of and feasibility for global consensus on shared values and virtues as human beings and institutions across cultures, religions and political systems. Based on this common ground it is then of course necessary to respect the diversity of local, continental, sectoral, religious and gender-related diversity.

5.5.3 Building trust by a balance of sovereignty and interdependency

Is the ethical answer to global disruptions and mistrust to slow down interdependency and digitisation? Or can Globalance be reached by convincing the competing superpowers that cooperation is still a better win-win than sanctions and exclusions? The exaggerated globalization 1990-2008 happened mainly under dominance of global multinational companies (MNC's) and the one superpower USA after the breakdown of the

Soviet Union and the bi-polar world. The shockwaves of the financial crisis 2007-2009, the populist and nationalist movements as counter-revolution to the globalisation revolution and now the Covid pandemic with the need for strong leadership of national governments led to propensity to reduce international dependency and increase national or even local sovereignty. The need is to balance both: We remain interdependent in a globalised world. We need global trade and investment for efficient resource allocation and production. We need scientific, cultural and religious exchange and cooperation for progress of humanity and for peace. However, we also need a sufficient level of sovereignty in decision for respect of the values of participation, freedom and human dignity. We also need it for adequate safety, protection and locally adapted solutions, as Covid shows.

The balance of sovereignty and interdependency means for Huawei, Tiktok and all other GAFA and BATH giant companies to continue their global footprint in a globalized world, but to strengthen the respect for national adaptation, diversification and control. Superiority attitudes, 'one wins all' strategies, submissive obedience to ill-intended directives from home or host regimes or circumventing national standards and orders with legal and tax tricks are counterproductive. These company leaders need not only a high level of technical and economic competence but a similar level of multicultural, multi-religious and political knowledge, sensitivity and respect combined with personal integrity![11]

Balancing sovereignty and interdependency in a healthy social and sustainable market economy also needs the avoidance of the monopoly relying on antitrust legislations. As it was implemented in the past hun-

[11] See Stückelberger, Christoph, *Integrity – the Virtue of Virtues*, in Christoph Stückelberger, Walter Fust, Obiora Ike (Eds), Global Ethics for Leadership. Values and Virtues for Life, Geneva: Globethics.net, 2016, 311-327. Free download www.globethics.net/publications.

dred years for several sectors such as banking, heavy industries or telecom, it has to be done related to the GAFA and BATH companies. In this respect, current legislative efforts of the US Congress to limit the accumulation of power of the GAFA companies and efforts such as from the European Union are ethically justified. They are needed in all markets in order to guarantee a fair market competition, across capitalist and socialist economies.

5.5.4 Building trust by common goals: fighting Covid and wars and supporting the SDGs

Let us rebuild trust by focusing on the common vision for humanity: a life in dignity, prosperity, sustainability and peace for all human beings in harmony with the whole creation. This vision is translated into the ambitious Sustainable Development Goals (SDGs), approved in 2015 by all nations of the world within the United Nations. The agreed target is to reach them by 2030. This is ambitious especially with the already visible backlash by the Covid pandemic where the poverty-wealth gap increases instead of decreasing (the billionaires increased their wealth during Covid from April to October 2020 by 25 percent, whereas the number of people in absolute poverty increases again, after a substantial period of decrease). The current US-China conflict for dominance is understandable from a superpower perspective (power deprivation rarely happens without violence), but it is deadly destructive. In such an extremely challenging time for humanity as the pandemic looms large, we need all energy for fighting the common enemy, which is this extremely tiny virus with the crown, called corona Covid virus (corona means crown in Latin). I am tempted to call it almost a crime against humanity if we now waste time and energy in the 'small' side-battles against single companies like Huawei or others from the GAFA and BATH 'families'. All sectors in all countries need now to stand together to fight the common tiny omnipresent enemy who claims to be the Cesar of the world with the crown: Corona Covid. In

addition, we need to be united in reaching the Sustainable Development Goals for a life in dignity for all.