ASIA PROGRAM

« SECURED PRODUCT » AND « TRUSTED COMPANY »:
LESSONS FOR THE DIGITAL SOCIETY FROM THE HUAWEI CASE

BY EMMANUEL MENEUT
PH.D, CATHOLIC UNIVERSITIES LECTURER

SEPTEMBER 2019

ASIA FOCUS #120

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

In February 2019, I wrote a note for the ASIA Focus1 on the use of drone as a tool for security about the terrestrial road of the OBOR project due to its connectivity. Hence, a drone manufacturer becomes a security provider because it determines the trustworthiness of the data flows and their accessibility. I took the case of DJI as the dominant market provider to illustrate the consequence : the "security challenge". Last month, on august 2019, the Department of Defense (DoD) has made a push to rebuild the industrial base to develop commercial drones that could be securely modified by the military for use on the battlefield. A standard for cybersecurity will have to be establish and trustfully followed by the manufacturers. Indeed, the Pentagon is worried that DJI shares data with the Chinese government. It has launched what is calling a "**Trusted** capital marketplace to connect **trusted** sources of capital with US small tech firms to catch up to China in the small drone market" where DJI get already a 2/3 market share. (SELIGMAN, 2019) A drone is a sample case of a connected object or the Internet of Thing (IoT) which is rising for the next decade if and only if, the communication network capacities will be upgrade to the "5G" technology. The prerequisite of the IoT or the "Digital society" is the deployment of the "5G" technology. The decision concerning the drone challenge is also the same structural challenge to promote domestic production of high tech components and products to counter china's technology explosion noticeably in "5G"[2]. Following the quotation made by the DoD, "trust" seems to be very important for the renewal of the industrial sector of small drone. I examine the role of this concept through the case of the "5G" challenge made by HUAWEI. The US made the decision to blacklist HUAWEI and banned US companies from selling technology to this firm because of the lack of trust toward HUAWEI "5G" components.

First, I will remind the features of this decision through the analysis of the presidential Memo : "Secure 5G". Second, I will articulate the initial view of J. Nye on cyber power

[1] Emmanuel Meneut, 28/2/2019, From safe product to secure product. A challenge for international relations: the case of drones, IRIS, at url: (https://www.iris-france.org/wp-content/uploads/2019/02/Asia-Focus-105.pdf)
[2] Lara Seligman, 27/8/2019, Pentagon seeks to counter china's drone edge, Foreign Policy

expressed in 2010 where "companies will comply with national legal frameworks rather than walk away from markets" with the view of J. Mearsheimer on loyalty to the state through his 2018 book "The great delusion" as the meaning of "trust". In the neoliberal approach, trust toward the manufacturer is resting only on product quality and safety. On the contrary, in the neo realist framework trust is a criterion to discriminate between a "secured product" and a product carrying political vulnerabilities.

The "Secure 5G - The Eisenhower National Highway System for the Information Age" Memo leaked in the press and was revealed by the WSJ in 2018. It is a ten pages Memo with a five slides presentation[3]. It is now available from the web site of the White House.

WHAT IS THE "5G" INFRASTRUCTURE ? A TECHNOLOGICAL BREAKTHROUGH

The "5G" network is a communication infrastructure, a network of information highways that increase the volume and the speed at which data may be exchange between connected electronic devices. It enables huge volume of information to travel at the light speed. It will increase the speed and quantity of data by **one hundred**.

This shift is a pre requisite to the digital society, especially the IoT centered on the connectivity of objects : from washing machine to airplane ! The data volume and speed will ensure that driverless cars don't crash, that machines in automated factories can communicate, etc. that "every device on earth will be real time wired together"[4]. As a consequence of the rapid diffusion of theses technologies, the number of connected devices will increase at an exponential rate. Actually, the leading companies of the digital sector will dominate the digital economy : the set of products and services using data from "5G" networks. They will be the global market players of the digital world. Today, HUAWEI is in a position to dominate the next generation "5G" technology : it controls 29% of the global telecom equipment market and 43% of the Asia-Pacific regional market[5].

[3] Jonathan Swan, David McCabe, Ina Fried, Kim Hart, (Jan 28, 2018) Scoop: Trump team considers nationalizing 5G network, AXIOS, consulted on 26/7/2019 à l'url: https://www.axios.com/trump-team-debates-nationalizing-5g-network-f1e92a49-60f2-4e3e-acd4-f3eb03d910ff.html

[4] Keith JOHNSON, Elias GROLL, (april 2019), The improbable rise of HUAWEI, Foreign Policy

[5] Ibid.

WHAT IS THE ISSUE OF THE "5G" INFRASTRUCTURE ? POLITICAL POWER

The main assumption of the Memo presentation is about communication infrastructure as **a key component of the power of a nation**. Both in term of capacities for military actions or "hard power" and values for influence strategies or "soft power". It is capacities for political actions, either black ops or public diplomacy to support US foreign policy and to provide domestic security for the American citizen. It is also capacities for the wealth production system, the economic activities. The 5G infrastructure is described as a structural factor of the American hard and soft power at a systemic and global level. The political issue of such telecommunication technologies for the cyber space is defined by J. Nye as cyber power. "it is the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power. Cyber power can be used to produce preferred outcomes within cyberspace or it can use cyber instruments to produce preferred outcomes in other domains outside cyber space."[6] The "5G" network, through the Internet of Thing (IoT) will tremendously expand the capacities to produce preferred outcomes outside cyber space, while the huge increase of information flows will unfold the capacities to produce preferred outcomes from public opinions within cyber space. The dominance of "5G" infrastructure provides hard power resources that can be used for sabotage and direct military attack and soft power resources[7] :

- the ability to make others do something contrary to their initial strategies, for example preventing dissident bloggers from sending their messages,
- the ability to set the agenda and exclude an actor strategy
- and the ability to shape another's initial preferences by delegitimizing certain ideas.

[6] Joseph NYE, (may 2010), Cyber power, Belfer Center at url: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf consulted on 26/8/2019
[7] Ibid.

Hence, from a political point of view, the "dependence on complex cyber systems for support of military and economic activities creates new vulnerabilities in large states that can be exploited by state and non state actors[8]."

The main barriers to tackle theses vulnerabilities are "redundancy, resilience and quick reconstitution which are the crucial components of defense[9]." However, they become out of reach without any capacities to control the physical infrastructure. The "Stuxnet" cyber-attack against the Iranian nuclear program infrastructures illustrates the difficulty. It took two years to the Iranian engineers to figure out their technical problems with the SIEMENS components of their infrastructure were not coming from mechanical defects or electronic failures. The "Stuxnet" cyber weapons, because of its intimate knowledge of the SIEMENS programming logic controller, was able to generate random cyber-attack to over speed the centrifuges until their destruction. The randomness of the destruction simulate operational failures. It made them undetected as cyber-attack[10].

Without any defense, a dependent state will have only one option to take advantage on its adversaries. He must practice a permanent offense in the cyber space. However, a "5G" cyber space under permanent fire of cyber weapons will preclude the Digital society and its economic benefits to spread globally. Nowadays, in the cyber space and the "4G" network, already the "offense currently has the advantage over the defense[11]". It is a strategic matter, which mobilize thousands of engineers and military men either in the US or in China. **Today, the digital economy** is facing the **cyber threat** as a key obstacle, both through the financial cost induced by safety and quality level required for the success of services and products based on Internet infrastructures : safety of personal data, financial transaction, etc. The "5G" network is a strategic opportunity to shift the digital economy at a much more important level of wealth production and to "solve" or mitigate the cyber risk. By producing a secured "5G" network infrastructure, a state gets a strategic advantage both in the military and economic sectors. It will shift significantly the balance of digital power.

[8] Ibid.
[9] Ibid.

[10] Isabelle LASSERRE (19/1/2011) La guerre secrète contre l'Iran retarde la bombe, le Figaro

[11] Joseph NYE, (may 2010), Cyber power, Belfer Center at url: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf consulted on 26/8/2019

This is a challenge for the US hegemony in the field of information and the cyber space. If China, whatever the means, is able to lead the "5G" technologies to deploy such network, at the beginning on its territory for its own population, taking account the size of the Chinese market, it means that China will dominate the "5G" sector and the digital revolution at the global level. The "5G" Memo **viewed China as the main competitor** of the US especially in the communication infrastructure domain. It has the "dominant position in the manufacture and operation of network infrastructure" and it is the "dominant malicious actor in the information Domain". (SWAN, 2018) Facing the threat to be overwhelmed, **the US must react**. As for the interstate or the space challenges, the US government should take the lead of this reaction.

WHY THE TECHNOLOGICAL CHALLENGE FOR THE US IS STRATEGIC ? IT WILL TAKE PLACE WITHIN 3 YEARS

This technological challenge with a political power issue is strategic because it will take place in a very short time. The "5G" Memo gave 3 years to the US government to tackle the Chinese dominance. Indeed, the S curve of the diffusion of a technology is a non linear phenomena. The diffusion of a technology takes place in a short period of time : "the world wide web begins in 1989. In the late 1990s, businesses begin to use these new technologies to shift production and procurement in complex global supply chains. In 1992 there were only a million users on the Internet, within fifteen years that had grown to a billion. In 2010 China alone had nearly 400 million users[12]."

As an illustration the following graph showed the rise of technological breakthroughs of the last century :

[12] Ibid.

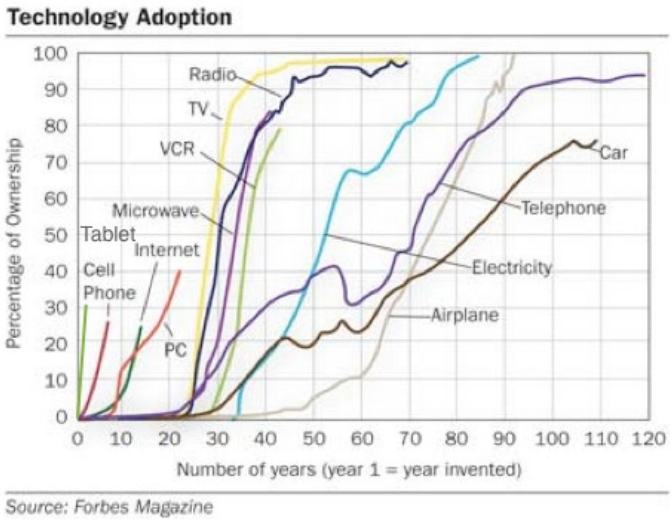


Fig. : the technological S-curve duration of a set of innovations

It is noticeable that from the Airplane to the Cell Phone, the number of years a technology takes to diffuse is shortening. It took two decades to the airplane to touch one third of the American population. It took a few years to the cell phone to reach the same share of the population. The speed of the diffusion is reducing for communication technologies. The same nonlinear and very rapid phenomena will take place with the new "5G" network. This situation is the result of the dynamic of a technological breakthrough, which followed an S-curve. It is permanent for each new technology; it is a structural feature of technological diffusion.

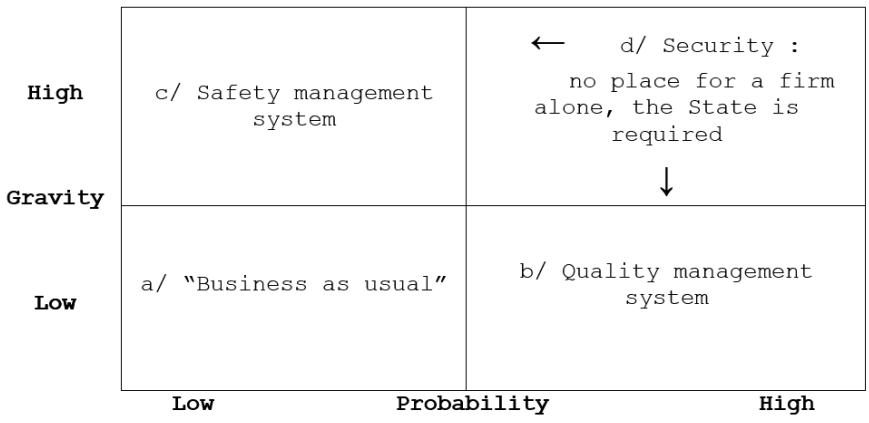
Hence, there is a veil of ignorance about security issues during the incubation phase of a technology. This mindset is quickly replaced by a strong requirement for security from the state. As soon as the car becomes the main transportation mean to go to work for the population, the oil dependence becomes a strategic challenge for the state. There is a necessity for the state and the firms to answer such challenge by fungible security means, most of the time based on force, money and intelligence. As illustrated by the US oil geopolitics in the Middle East since 1945. When driverless cars will replace today's car, the "5G" network security will be a critical security issue. It is a strategic matter. The short

duration of the diffusion phase is an amplifier of the security challenge. The more rapid is the diffusion, the more pressing is the security issue.

Actually, the security requirement is coming from public opinion. Any car user must be sure he will have access to the fuel his car needs at any gas station on the territory. The probability of rupture must be acceptable; it should be very low, for example after a devastating hurricane and not a rainfall. Hence, the state and the firms develop risk management processes and tools to reach an acceptable risk level for the public opinion. Driverless cars will have to be quality products, for instance comfortable but also safe products, not killing its passengers and intelligence agencies would not get access to data flows and commands.

WHAT ARE THE FEATURES OF THIS SECURITY CHALLENGE ? THE STATE AND THE FIRMS

From a company point of view in a market economy, classical risks management is drove by two independent variables, the frequency of undesired events and their gravity. Actually, they defined four spaces for the risks management process :



The low probability and low gravity situation defines a space (a/) where a firm could provide mass products or services without high level of cost to support a quality or safety

management system. It is the economic area where business drivers are the price and the cost criteria. For example, it was the case for car mass production of the 1920s and the 1950s.

The high probability and low gravity situation defines a space (b/) where a firm should invest into a quality management system to support mass production in order to satisfy its stakeholders. It was the case of the Japanese car industry during the 1990s.

The low probability and high gravity situation defines a space (c/) where the firm must invest into a safety management system to support its business processes, usually it is a requirement by the State in order to gain social acceptance of the economic activity. For instance, it is the case of the nuclear and airlines industries.

Finally, the high probability and high gravity situations defines a space (d/) where a firm could not survive. The firm reputation could not sustained regular catastrophic events such as high rate of driverless car accidents. Each time an activity fall within this area, a **security challenge** must be address in order to develop a profitable business field. Either the frequency or the gravity should be reduce, most of the time both dimensions will be address by the State and the firms. A product failure must be rare. In the case of cyber-attacks, the security challenge could only be meet by a State actor with sufficient fungibles means to mitigate the risk (force, money, intelligence). A firm is a specialize actor without access to all the fungibles means required to tackle numerous catastrophic cases.

Hence, the security challenge required the state to articulate the risk management process of the firms and the risk acceptability from public opinion. This security challenge is noticeable from the "5G" Memo : "The advent of secure network technology and the move to 5G presents an opportunity to create a completely new framework to safely, securely and reliably transport and share information… The next generation technology… can position the US to leap ahead of global competitors and provide the American people with a secure and reliable infrastructure to build the 21st century equivalent of the Eisenhower National Highway System, a single, inherently protected, information transportation superhighway." (SWAN, 2018) There is a recurring use of the "security" semantics.

On the contrary of the Al Gore discourse during the 1990s to favor the development of information super highways where the cost efficiency was the main criteria… may be because most of the telecommunication companies were American ! "We have a dream for…an information superhighway that can save lives, create jobs and give every American, young and old, the chance for the best education available to anyone, anywhere[13]."

A safe product is not dangerous and a quality product is an efficient one. The US/China confrontation is now structured by the ability to provide secure "5G" network to its people.

SO, WHY IS THERE A PROBLEM ? BECAUSE OF THE LACK OF TRUST BETWEEN THE US GOVERNMENT AND THE CHINESE FIRMS

The HUAWEI threat perception by the US is both economic and politic. The economic feature of the threat are the market share, the price war strategy, the technological quality, the R&D financial support. But these economic dimensions are not the main obstacle of the security challenge. From the market economy theory the main variable for interdependence is the **comparative advantage** between manufacturers. If a firm is able to produce goods or services at better **quality** and affordable price one should thank competition and free trade and buy such a product. If a product is of quality, if it is **safe**, it doesn't hurt anyone, no one should preclude a consumer to buy it. HUAWEI product are quality products at good prices and they are safe. Nowadays, most of the components for a quality and safety 5G network are designed and assembled by Chinese firms or come from HUAWEI and ZTE.

The "5G" Memo described the Chinese "5G" network manufacturing based, mainly HUAWEI and ZTE, as a threat to the American power. Then it described the decisional

[13] Gil Press, (11/1/2016) Al Gore Invents The Internet: This Week In Tech History, FORBES

situation and provided options to the president. Under the Chinese threat, the US government may seize this opportunity and provide a global plan within a three years strategic window. The main question for the president is which role distribution between the US government and the American private manufacturing base.

Hence it is another dimension which intervene in the threat perception. Because these products are related to information or soft power ; they must also be **secure for the US government**. But what does this mean ?

WHAT IS HUAWEI ? A CHINESE GLOBAL FIRM

HUAWEI was founded in 1987 and today it is the first company on the telecommunication network products global market. This success story has been possible because of the weakness of the Chinese legal framework on intellectual property, the strong cooperation with its contractors and sub-contractors, the financial support of the Chinese state, around $10 billion and public contracts[14]. HUAWEI may have received $30 billion from the China Development Bank[15]. HUAWEI reached this dominating position on the Chinese market and then at the global level. HUAWEI is the first company for telecomm infrastructure : antenna, radio stations, optic fiber communication, software platform, cloud technology. It is vertically integrated. It designs every component of 5G technology. Its 2018 benefits are $8.8 billion. It is the world largest telecom equipment company, $107 billion in revenue from operation in more than 170 countries[16].

[14] (Xavier SEURRE, 2019, L'intelligence artificielle : enjeu stratégique pour la puissance chinoise, Mémoire de Master, ICP-FASSE)

[15] Keith JOHNSON, Elias GROLL, (april 2019), The improbable rise of HUAWEI, Foreign Policy

[16] Ibid.

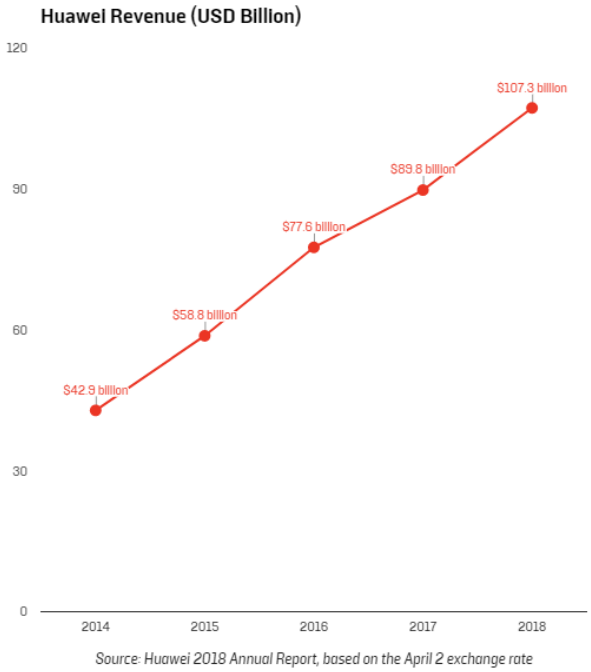


Fig. : HUAWEI Revenue[17]

Its annual R&D budget is around $15 billion, it has 14 R&D centers and around 80 000 engineers dedicated to R&D. It has always been the strategy of HUAWEI to develop its own technology. In the 1990s the company have had 500 R&D staff and 200 in production[18]. It is the most important company in term of intellectual property; it was the first company to file patents in 2018, since 3 decades it owns more than 87 805 patents[19]. HUAWEI owns 1 529 essential "5G" patents and ZTE owns 1 208 compared with Nokia 1 397 and Ericsson 812. The first American company, Qualcomm, owns 787 essential patents and Intel 550.

[17] Keith JOHNSON, Elias GROLL, (april 2019), The improbable rise of HUAWEI, Foreign Policy
[18] Ibid.

[19] (Xavier SEURRE, 2019, L'intelligence artificielle : enjeu stratégique pour la puissance chinoise, Mémoire de Master, ICP-FASSE)

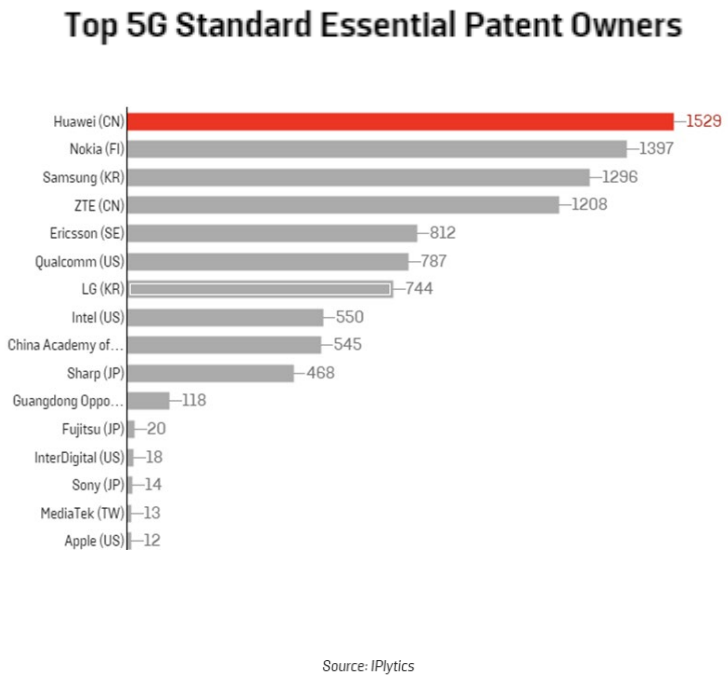


Fig. : HUAWEI patents[20]

HUAWEI made 11 423 technical contributions to the "5G standard and Ericsson 10 351, Qualcomm 4 493[21]. HUAWEI's leading role in shaping technology standard will likely give the Chinese firm an advantage to dominate foreign markets. HUAWEI provides cutting edge technology of its own which frame the future of the "5G" technology at the global level.

[20] Keith JOHNSON, Elias GROLL, (April 2019), The improbable rise of HUAWEI, Foreign Policy
[21] Ibid.

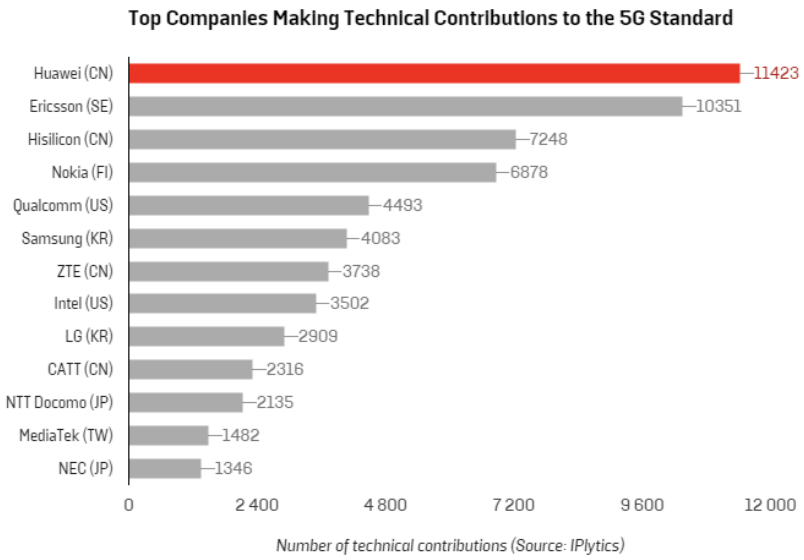


Fig. : HUAWEI technical contributions to 5G standar[22]

This path rested on classical governments' levers used by most of western companies, like Boeing in the field of aeronautic manufacturing.

The lack of trust toward Chinese dominant suppliers is creating a security threat perception between Beijing and Washington. The informational hegemony of the US and its soft power is directly challenged by the technological power of Chinese companies. Even if using these suppliers make good economic sense, a political dimension bared any partnership between the US government and the Chinese firms. So, why president Trump couldn't **trust** the products quality and safety from HUAWEI as he trusts CISCO or VERIZON or QUALCOMM or SPRINT or TMOBILE products and services ?

[22] Ibid.

HOW TRUST WORKS BETWEEN A GOVERNMENT AND A FIRM ? THROUGH THE LEGAL FRAMEWORK AND LOYALTY TO THE STATE

The cyber space may be viewed as an "hybrid regime of physical and virtual properties. The physical infrastructure layer follows the economic laws of rival resources and increasing marginal cost, and the political laws of sovereign jurisdiction and control. The virtual or informational layer has economic network characteristics of increasing returns to scale, and political practices that make jurisdictional control difficult[23]."

Hence, it is not surprising that HUAWEI and ZTE become the global companies that provide physical layer of the next "5G" generation of the cyber space, based on classical business strategy of quality and safe products at affordable prices. However, it gives access to the Chinese state apparatus to the political practices within their territories, but also outside their home country.

This **political levers** rest on the Chinese legal framework at home and on the **trust** between the state and the management of these companies outside China. The management loyalty toward the state will have to be unique and total. For example, "Hong Kong airline Cathay Pacific's CEO stepped down in august 2019 after some of its staff were reportedly involved in the democracy movement. It is rumored that the resignation came because he refused to hand over the employees' names to the Chinese authorities, though reports are unconfirmed. The turmoil at Cathay Pacific comes amid reported threats against the Big Four accounting firms in Hong Kong for not sufficiently supporting Beijing[24]."

The key variable of the strategic advantage a state get from producing the components for the "5G" infrastructure is the legal framework of the companies and the loyalty of its management and employees toward the state. "Governments can bring physical coercion to bear against companies and individuals, what has been called the hallmark of traditional legal systems[25]." But even the legal framework required loyalty to the state.

---

[23] Joseph NYE, (may 2010), Cyber power, Belfer Center at url: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf consulted on 26/8/2019

[24] James BALMER (21/8/209), Decoding China's 280-character web of disinformation, Foreign Policy

[25] Joseph NYE, (may 2010), Cyber power, Belfer Center at url: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf consulted on 26/8/2019

Recently, a lot of American employees are shaking their companies when they are working for the US government because of its political goals. Those American companies, like the communication agency Ogilvy are focusing on their customers goals, the new migration policy, and the trust of their customers, the Custom and Border Protection, in the high degree of confidentiality it will benefit even when it is clearly against their deepest human values as Ogilvy CEO John Seifert explained : "as a person who, my first wife was Mexican American, both of my sons are fifty percent Mexicans as far as I'm concerned. I find what is going on in the immigration debate broadly and what is going on in particular in terms of the horrific human situation going on at the southern border abhorrent[26]." Even with such antagonism, the Ogilvy CEO and its employees are serving the Custom and Border Protection goals with the highest level of confidentiality.

More than the legal framework, loyalty to the state is at stake. It is not simply a matter of legal framework but mostly of citizenship. If HUAWEI engineers are loyal to the state, as the CISCO engineers, what will happen when their respective governments go to a confrontation ? The international relation dimension may become a matter of **political loyalty to the state**.

WHY LOYALTY TO THE STATE IS THE MOST IMPORTANT FACTOR ? FOR SECURITY PURPOSE

Indeed, the legal framework works only when it is a matter of economic activities. The "legal prosecution made Yahoo control what it sent to France and Google removed hate speech from searches in Germany. Even though the message were protected free speech in the companies' home country, the US. The alternative to compliance was jail time, fines, and loss of access to those important markets[27]." But this mechanism doesn't work when the companies are HUAWEI and ZTE and the foreign market is the US. The main reason is

[26] Lam THUY VO, Nancy VU, (Juillet 2019) transcript shows how Trump's border camps have thrown a top advertising firm into internal crisis, BuzzFeednews, consulté le 6/82019 à l'url: https://www.buzzfeednews.com/

[27] Joseph NYE, (may 2010), Cyber power, Belfer Center at url: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf consulted on 26/8/2019

not the legal framework, it is the lack of trust toward the HUAWEI manager by the American security apparatus.

To satisfy the demand of law enforcement, telecommunication networks are built to enable wiretapping and interception functions. They are used by intelligence agencies to collect data. National government manage security matters : espionage, crime, influence, within national legal frameworks. The need for security required loyalty to the state in the legal framework of a firm, which focused on the result. Political pressure exerted through intelligence agencies that inserted back doors and Trojan horses into components have no vested interests in global markets[28]. They required trust and foremost discretion at the edge of the legal framework.

Even in a liberal society, the executive power will look for a legal framework which enable to get result efficiently in the field of security. "General M. Hayden, who led the NSA on 9/11 and later took over the CIA, was found of saying that in carrying out intelligence activities he has a duty to play aggressively right up the line : playing back from the line protected me, but didn't protect America. I made it clear I would always play in fair territory, but that there would be chalk dust on my cleats. Against a merciless enemy, we fight hard. I don't apologize for that. But we fight within our laws[29]." The consequence of "playing right up the line" is the requirement for capacities to implement what is needed within the communication infrastructure components, either hard or soft, to get the results. The communication companies are concerned by such cooperative behavior.

The liberal state worked out the security challenge in the framework of the rule of law which is oriented toward efficiency and results. "During W Bush second term, the Time revealed the warrantless surveillance program. It prompted a flood of litigation against the NSA and the telecommunications companies that had secretly provided the agencies with access to their customer's private information without warrants. A federal district

[28] Elisabeth BRAW, (April 2019) The manufacturer's dilemma, Foreign Policy

[29] Charlie SAVAGE, (2011), Power wars, inside Obama's post 9/11 presidency, Little, Brown and Company

court judge ruled that the program was illegal because it bypassed congressional regulation and court oversight. During Obama first term, Congress enacted a law authorizing the warrantless surveillance program and bringing its general administration under the oversight of an intelligence court[30]."

The ability of the intelligence agencies to trust the engineers of the telecommunication companies is a prerequisite of the efficiency of the security policy. Especially when intelligence agencies specialist turn around between public organization and private companies during their career as illustrated by the E. Snowden CV !

This is exactly what is at the origin of the threat posed by HUAWEI : it works with the APL, the Chinese intelligence agencies and the state (Guoanbu). HUAWEI engineers are loyal to their state. The Chinese intelligence legal framework for surveillance of 2017 requires any company to transfer all personal data to state security departments about anyone or any organization included data from outside the Chinese territory. Hence, the Chinese security state apparatus is efficient and focused on the results as the American one. There are strong links between HUAWEI, the APL and the Chinese intelligence community[31].

This state of affairs is similar to the one in the US where American companies evolve within a legal framework where the intelligence agencies developed working processes at the limit to get what they need to provide security. It forbids any trust from the US government toward Chinese companies. The origin of the **digital security dilemma** between China and the US is the lack of trust between the American state and the Chinese companies' management and employees. The impossibility to trust Chinese designed equipment for "5G" network triggered a security dilemma where the main alternative for Washington is to "invest $200 billion to build its own "5G" secured network in 3 years, as recommended in the "5G" Memo or to acknowledge the leading role of China in cyber power. The issue is the capacity to monitor its population and to spy on rival nations and steal their strategic secrets. American principal deputy director of national intelligence

[30] Ibid.
[31] Keith JOHNSON, Elias GROLL, (april 2019), The improbable rise of HUAWEI, Foreign Policy

Sue Gordon and US intelligence officials are already beginning to prepare for a world in which HUAWEI dominates next generation telecommunications networks : "we are going to have to figure out a way in a 5G world that we're able to manage the risks in a diverse networks that includes technology that we can't trust"[32]

If HUAWEI is a key asset to the Chinese power and survival of the regim, Chinese engineers will not make defection when they will be ask to workout a solution in security mater. The "Raison d'Etat" will prevail, whatever the legal framework. Trust, as loyalty to the state is the key lever to secure digital product. Nationalist "state want their people to be as united as possible and feel loyal to the state[33]". A nationalist state builds "loyalty between the people and their rulers[34]". When people are strongly bond together by national link, there are much less defection to the national interest or the security decision made by the government in order to favor the survival of the collective group and the polity : "desertion is much less of a problem when soldiers are drawn from a nationalistic population[35]."

On the contrary, the neutral "state of the liberal society doesn't favor emotional attachment to the state among its citizens. It is hard to motivate people to fight and die for a liberal society[36]." At the extreme, "liberalism undermine social cohesion and nationalism creates strong bonds between individuals and their state[37]" Hence, liberal society confronted to security challenge will develop a double command posture to promote its security interests under the umbrella of a free trade and open society discourse.

Actually, what is at stake is the inability of the US government to trust HUAWEI as a company which is simply serving its customers. This inability is coming from its own "**double command**" behavior. The free trade discourse and the use of non-economic levers, the dollar diplomacy or the extra territoriality of the US law, the economic intelligence provided by the intelligence agencies to American firms to increase market share abroad and to eliminate competitors, etc. The basic strategies of the economic war.

[32] Keith JOHNSON, Elias GROLL, (april 2019), The improbable rise of HUAWEI, Foreign Policy
[33] John MEARSHEIMER, (2018) the great delusion: liberal dreams and international realities, Yale University Press
[34] Ibid.
[35] Ibid.
[36] Ibid.
[37] Ibid.

If the US implements such practices, the Chinese government will also take advantage of its new intelligence capacities coming from the HUAWEI leadership on the "5G" network. In comparison, the management of facilities and support budget of the American intelligence agencies is around $14 billion mainly performed by the National Security Agency which provides the interception infrastructure. The consequence of the HUAWEI today's technological and financial capacities ($107 billion of revenues, $14 billion of R&D and 80 000 research engineers) is a strategic autonomy of the Chinese State to develop its own digital "practice" to sustain its competition with the US. President Trump is simply reminding everyone that a company, its CEO and its employees have a political loyalty to the rules and the rulers. The confrontation between Washington and HUAWEI illustrates that a company doesn't have the choice between compliance to the legal framework or walk away a potential market. In the digital society, the trust toward companies, in term of political loyalty is the critical question. The HUAWEI case remind us that "from the American point of view Twitter and YouTube are matters of personal freedom, seen from Beijing or Teheran, they are instruments of attack[38]."

Secure products is the answer to this challenge. Actually, a **secure product** is a product coming from a trusted company. A a trusted company is one with a clear loyalty to one state. A trusted company is a company which is able to work at the limit of the legal framework, like the whistleblower Edward Snowden revealed concerning the generalization of surveillance of any citizen American or not by the US government with the help of the American telecommunication companies. Hence, a secured product is designed only for a specific market under the control of a particular state with exclusion of others. Following D. Drezner typology, high conflict between digital great power unfold either a "sham standards" (censorship) or "rival standards" (consumer privacy) regim[39].

[38] Joseph NYE, (may 2010), Cyber power, Belfer Center at url : https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf consulted on 26/8/2019
[39] Daniel Drezner, (2004), The global governance of the Internet: bringing the state back in, Political science quaterly, vol. 119 n°3

The former is characterized by a prominent role either to the government or IGO/NGO and the later by a dominant role of the government. Both featured no stable coordination :

Great Power Distribution of Preferences	*North/South Distribution of Preferences*	
	High Conflict	*Low Conflict*
High Conflict	*Sham standards* (Censorship)	*Rival standards* (Consumer privacy)
Low Conflict	*Club standards* (Intellectual property)	*Harmonized standards* (Technical protocols)

Fig. : typologie of Internet governance issues followed D. Drezner

The challenge posed by China to the US is the lack of "hard power" lever to force China to seat at the negotiation table with the need to find a compromise either "club" or "harmonized" standards ; to the contrary of Japan in the 1980s about electronic technology. The cyber space regim "of loosely coupled norms and institutions somewhere between integrated institutions that imposes regulation through hierarchical rules and highly fragmented practices and institutions with no identifiable core and nonexistent linkages" is no more an option for the digital society[40]. It will be fragmented markets.

Indeed, security is the main obstacle and it is a challenge for the state as the main security provider. The complexity and the speed of the "5G" diffusion will require from the state the devolution of some cyber security responsibilities and authority to private actors. The first difficulty is coming from the level of political power the state may transfer to private companies : "corporation aggregating and monitoring the data exchanged by individuals

[40] Joseph NYE, (may 2010), Cyber power, Belfer Center at url: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf consulted on 26/8/2019

wield powers of influence and surveillance exceeding those of many contemporary states and of even more tradition powers. And governments, wary of ceding the new field to rivals, are propelled outward into a cyber realm with as yet few guidelines or restraints. As with any technological innovation, the temptation will be to see this new realm as a field for strategic advantage[41]." Moreover, it will not contribute to the reinforcement of transnational private actors to manage a global commons.

Security of the next generation cyber space or "5G" infrastructure is a structural challenge. The devolution problem, the transfer of security functions to non state actors, cannot be tackle only at the firm level with a legal framework focused on quality and safety only. Indeed, if a company wants to secure its suppliers it must manage risk of its direct suppliers but also its sub contractors which number rises at an exponential rate due to the structure of the web of the global supply chains. A firm with 5000 direct suppliers, each with 250 sub contractors is growing to 1.25 million second tier supplier. In software and electronic engineering, backdoors, Trojan horses, clock bomb are weapons an intelligence agency could easily introduce within such number of suppliers. One subverted supplier is enough, quality, safety and security rest on testing and quantitative measures which are out of reach. Security at last is a matter of trust. The structural impossibility to secure all the components of a 5G network is a permanent vulnerability for each digital great power. None can left the other to dominate the "5G" infrastructure. There is no possibility for a firm to manage the security issue at its level. Security is a systemic property, it is an environment feature. As illustrated by the Edward Snowden case on how American companies were "forced" to cooperate with US intelligence agencies. Trust must be established at the political level from the education system, to the socialization institution and the legal framework of the society. As H. Kissinger noted : "the dilemma of such technologies is that it is impossible to establish rules of conduct unless a common understanding of at least some of the key capabilities exists. But these are precisely the capabilities the major actors will be reluctant to disclose. The US has

[41] Henry KISSINGER, (2014), world order, reflection on the character of nations and the course of history, Penguin Book

appealed to China for restraint in purloining trade secrets via cyber intrusions, arguing that the scale of activity is unprecedented. Yet to what extent is the US prepared to disclose its own cyber intelligence efforts ?[42]" As a consequence, a company's management and employees loyalty toward one state becomes the critical political variable of the emerging digital society. It is a structural digital security dilemma.

[42] Ibid.

ASIA FOCUS #120

« SECURED PRODUCT » AND « TRUSTED COMPANY »: LESSONS FOR THE DIGITAL SOCIETY FROM THE HUAWEI CASE

BY EMMANUEL MENEUT / PHD, CATHOLIC UNIVERSITIES LECTURER

SEPTEMBER 2019

ASIA FOCUS

Collection supervised by Barthélémy COURMONT, research director at IRIS, lecturer at the Université Catholique de Lille, and Emmanuel LINCOT, professor at the Institut Catholique de Paris – UR "Religion, culture and society" (EA 7403) and Sinologist.

courmont@iris-france.org – emmanuel.lincot@gmail.com

ASIA PROGRAM

Supervised by Barthélémy COURMONT, research director at IRIS, lecturer at the Université Catholique de Lille.

courmont@iris-france.org

THE FRENCH INSTITUTE FOR INTERNATIONAL AND STRATEGIC AFFAIRS
2 bis rue Mercoeur
75011 PARIS / France
T. + 33 (0) 1 53 27 60 60
contact@iris-france.org
@InstitutIRIS
www.iris-france.org