ISPI DOSSIER September 2020

THE GEOPOLITICS OF 5G

edited by **Samuele Dominioni, Fabio Rugge**

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

September 2020

5G technologies are reshaping the way users experience the digital sphere and, thus, their daily lives. 5G is one of the game changers that would further enable cyberspace's potentialities for our societies, economies, and lifestyle. Yet, there are multiple and contrasting geopolitical interests and security concerns regarding 5G adoptions and implementations. The current confrontation between Chinese companies and some Western governments is emblematic. What are the political and securitarian implications of such technological disputes? How are states dealing with the security of 5G technologies?

** Samuele Dominioni is a Research Fellow at the ISPI Centre on Cybersecurity, in partnership with Leonardo.*

** Counselor Fabio Rugge is Head of ISPI's Centre on Cybersecurity, in partnership with Leonardo. He is a diplomat currently working as Head of the Office in charge for NATO and Security and Politico-Military Issues, Directorate General for Political Affairs and Security, Ministry of Foreign Affairs and International Cooperation.*


4G
5G

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

September 2020

5G in a Contested Domain

Fabio Rugge
MAECI, ISPI

The international debate regarding the acquisition of Chinese 5G technology appears symbolic of the re-emerging Great Power Competition, and stark proof of the ongoing decoupling of the global ICT supply chain. Washington has been pressing its allies for more than a year not to adopt Chinese 5G technology and threatened drastic cuts in intelligence information-sharing with those procuring it. We cannot ascribe these developments to Washington's hidden market-share considerations, as the US market does not yet offer a competing technology, nor can we consider them yet another example of President Trump's tough positions on trade negotiations, especially with China, because it is since 2012 that the US Administration has prohibited several government agencies, on the grounds of "national security risk", from acquiring products from Huawei and ZTE, two of China's most successful high-tech exporters. Is Chinese 5G technology so dangerous, and if so, why is the ban on Chinese 5G technology so contentious?

Fabio Rugge is Head of ISPI's Centre on Cybersecurity, in partnership with Leonardo. He is a diplomat currently working as Head of the Office in charge for NATO and Security and Politico-Military Issues, Directorate General for Political Affairs and Security, Ministry of Foreign Affairs and International Cooperation.

5G networks will enable the Internet of Things revolution, which, together with the exponential progresses in computing power and advances in AI, will transform our everyday life in ways we can barely imagine. 5G networks will represent the nervous system connecting the political, strategic, military, informative, economic, financial, industrial and infrastructural dimensions at a personal, local, national, international and transnational level. In this scenario, there are at least three categories of risks that might arise from relying upon untrusted 5G networks. The first is the "classic" risk of espionage by foreign entities (be they governmental or private companies subject to a strong government's direction), targeting governments' confidential information, commercial or industrial secrets, our personal lives. This would certainly pose a direct threat to our freedom, to our independence and to our welfare. A 5G controlled more or less directly by foreign entities would also give them the power to profile users, to manipulate data and divert data flow, and eventually to influence our individual perceptions and our public opinions. Cyber-enabled information warfare already appears to be one of the instruments of choice in the ongoing international confrontation, and it has proven its destabilizing potential in several international crises. Developments in deep-fake technology and in "automated propaganda" will certainly elevate the threat even further. Finally, in time of crisis, an untrusted provider might use the network to exert political and economic pressure and to acquire a military advantage, for instance if its operators denied an essential service to a critical national infrastructure, or if it voluntarily provided forged data, or sabotaged essential democratic or industrial processes, or hampered political decision-making on issues of national security and defence.

Against this backdrop, policy-makers must decide whether to allow Chinese off-the-shelf providers to prevail or if it is more appropriate to delay the fielding of 5G in order for trusted vendors to be able to offer a safer and more secure alternative. It is indeed an unprecedented dilemma for our policy-makers, accustomed to a Western technological superiority that is now increasingly challenged in every domain, and to free-market dogmas that mandated the globalization of supply chains. Responses have so far been diverse. Some Western countries delayed the acquisition of 5G technology altogether, while some others tried to distinguish between "core" and "non-core" parts of the networks, assuming it will be possible to procure Chinese 5G technology for the latter. Some states, also, decided to impose specific security standards for ICT components for specific sectors of national security importance. Many others have yet to say the final word, and have so far changed their position a few times.

National security concerns normally prevail without too much hassle over market or economic development considerations, especially where there is so much public attention. The issue of Chinese 5G, on the other hand, seems to be of a different kind. Is it because the West cannot accept delaying the digital transformation enabled by 5G, no matter what? Is it because of the very significant

investments that Chinese providers are willing to make in Western infrastructure? Or is it because, after Snowden's revelations, the public opinions of Europe believe that, since everyone hacks, it does not really make a difference who to trust, especially in the absence of concrete proofs that the Chinese government used its ascendancy over Huawei and ZTE to hack data? Maybe the answer is a combination of both these reasons, or maybe the fact is that there is simply a general lack of awareness about the threats stemming from cyberspace, and possibly also about the reasons, the bearings and the practical implications of the ongoing new Great Power Competition.

This lack of awareness is understandable: cyberspace is the domain of ambiguity, where it is impossible to understand and anticipate the motivation and the scope of a cyber campaign without considering the strategic, political and operational context in which it occurs. The difficulty in attributing the cyberattacks, together with the widespread recourse in cyberspace to falsely flag computer network operations, make it difficult to know "what is really going on" in the cyber domain, and to make sense out of it. Cybercrime, hacktivism, intelligence and military computer network operations, all share the same domain and they all use the same tactics, techniques and procedures, and they all exploit the same vulnerabilities. Cyberspace has therefore become the domain of choice for destabilising campaigns and engaging in hostile activities that would be simply unsustainable in the conventional realm. National intelligence communities usually are better placed and equipped to handle sensible information and grasp the complexity "behind the curtains" of the ongoing confrontation in the cyber domain – but this is also another reason why an in-depth understanding of cyber affairs is not easily accessible to the general public, or even at the institutional level.

If what happens "in and around" cyberspace is already difficult to know and to understand, and much harder is to picture how the world will transform in just a few years given the rapidly of technological progress, what complicates the picture even further on the issue of 5G is the traditional unfamiliarity of public opinions with matters of foreign affairs and international security. Questions of international security are rarely on the top of the political agenda or make headlines, and world public opinions do not seem very much concerned about the resurgence of the Great Power Competition or the comeback of strategic instability. It is little wonder, therefore, that the ongoing decoupling of the global ICT supply chain does not attract great attention outside of specialists' circles. It is, instead, a crucial development in today's international security environment.

We are undergoing a digital revolution that has already brought about paradigmatic changes to the theory and practice of international security – and we are just at the beginning. Progress in the field of Artificial Intelligence, for example, will soon permit the automation of weapon systems (even those of cyberspace) and the most efficient planning of operations; it will allow public opinion to be manipulated far more effectively through deep-fakes and cyber-enabled information warfare, and will

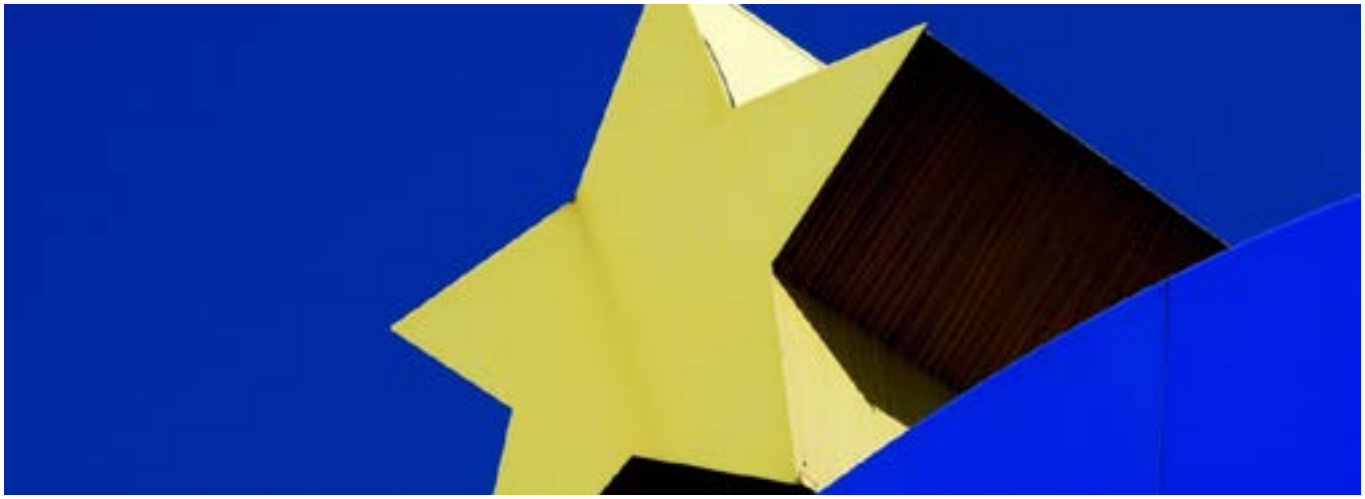
exponentially increase the speed of future conflicts. Tomorrow's hyperwars will be fought by machines with autonomous decision-making capabilities; "algorithmic warfare" will become the norm. In this new strategic environment, it is more important than ever to maintain the technological superiority historically associated with the Western hegemony over the international system, which is now threatened by the advance of political models alternative to, and in direct competition with, the West.

Mobilisation to maintain technological and cyber superiority is at the origin of the ongoing global decoupling of the hardware and software ICT supply chains. It is also provoking the gradual building of barriers to technology transfer and the proliferation of national safeguards against foreign technological products and services, resulting in a global normative patchwork. Not only in the West: Beijing, for instance, recently decided to replace all the hardware and software used by public bodies with domestically-produced technology. In this competition between Great Powers, even Internet traffic is segmented by different, interconnected – but, if necessary, independent - systems: China erected its Great Firewall, and Russian networks can now, by law, be segregated in case of need. These developments are the result of competition between opposing blocks, and they simultaneously intensify that same competition.

The more important privacy, accessibility and integrity of data become to national security, the more urgent it is for states to bolster cybersecurity and the more potentially advantageous offensive actions in cyberspace and on the ICT supply chain become. Cyber power and the control over ICT networks and data are hence simply another dimension of 21st century sovereignty. In this sense, even if the Chinese 5G connectivity were demonstrated to be safe, secure and reliable, it will grant Beijing a valuable access to data which is, in itself, an enabler for cyber power. In times of Great Power Competition and digital revolution, this might be problematic.

ISPI
ITALIAN INSTITUTE
FOR INTERNATIONAL
POLITICAL STUDIES

September 2020



What Does the EU Say About 5G?

Corrado Giustozzi
ENISA and AGID

It is commonly believed that 5G networks will allow the development of new types of services based on innovative use cases, for the benefit of both private end users and companies, thus becoming the real "nervous system" of the future connected society. This will also have obvious positive effects on the economy: the European Commission estimated that 5G will generate a turnover of 225 billion euros in five years, and the related networks will be used by 2.6 billion users worldwide, that is 40% of the total world population. As early as 2016, the Commission adopted the 5G Action Plan to make sure that the Union has the connectivity infrastructure necessary for its digital transformation as of 2020, and for comprehensive deployment in urban areas and major transport paths by 2025[1]. This action plan set out a clear roadmap for public and private investments in 5G infrastructure in the EU.

On the other hand, making 5G networks a crucial infrastructural component for digital society in the coming years in turn brings

Corrado Giustozzi, Cybersecurity expert at Agenzia per l'Italia Digitale (Agency for Digital Italy) for the development of the governmental CERT for the Public Administration (CERT-PA). Member of the Permanent Stakeholders' Group at ENISA (European Union Agency for Network and Information Security). Member of the Board of Directors at Clusit (national italian association of information security professionals).

attention to the enormous risks arising from possible malfunctions and abuses, especially of a malicious and intentional nature, to which they are subject. Most of the concerns come from the substantially new implementation paradigms of 5G networks, and from the extreme complexity of the hardware and software components on which they are based.

This scenario has led many governments, as well as their respective national and supranational regulatory authorities, to undertake careful preventive analyzes of the possible risk profiles related to the various scenarios of use of 5G, in view of the issuance of rigorous technical standards and safety measures. In fact, the EU considers it of paramount importance to ensure the security and resilience of 5G networks by adopting a common and balanced approach among member states.

Therefore, in March 2019 the Commission published a first recommendation[2] regarding the cybersecurity of 5G networks and then, a few months later, published a report[3] in which the main cybersecurity risks in 5G networks were identified and analyzed. They were: an increased attack surface consisting of potential vulnerabilities in the software used to implement the core and service components of the networks; problems of sensitivity and interoperability at the hardware level due to the particular architecture and new functions of the networks; increased exposure to attacks due to the risk profile of a supplier or manufacturer, as well as the dependence of mobile networks and enterprises on a third party supplier or manufacturer; IT network-level threats that compromise the availability and integrity of 5G networks that act as a backbone for mission-critical applications.

Following those studies, early in 2020 the Commission published the so-called "EU Toolbox"[4], a set of measures specifically developed to mitigate the cybersecurity risks of 5G networks identified at national and EU levels; it was backed by a Communication[5] which required all member states to take steps to implement the set of measures recommended in the Toolbox by 30 April 2020, and to prepare a joint report on its implementation by 30 June 2020.

The Toolbox identified and provided risk mitigation plans for each of the nine risk areas identified in the EU coordinated risk assessment document. Its goal was to create a robust, coherent and objective framework of security measures, at both the strategic and technical levels, in order to ensure an adequate level of cybersecurity of 5G networks across the EU. From this standpoint, a shared strategic view and a coordinated approach among member states are fundamental: in particular, the member states agreed to ensure that they would be able to restrict, prohibit, and/or impose specific requirements and conditions, in accordance with a risk-based approach, for the supply, deployment, and operation of 5G network equipment.

On 24 June 2020 the Commission released the report[6] on the progress made by the member states in implementing the Toolbox. The results are considered quite good in most areas,

although a few aspects of the Toolbox are not fully covered yet and need some further work. One important point concerns the powers of national regulatory authorities in the member states: most of them have been or are in the process of being reinforced, to regulate both 5G security and the procurement of network equipment and services by operators. Measures aimed at restricting the involvement of suppliers based on their risk profile are already in place in a few member states, and at an advanced stage of preparation in many others. Network security and resilience requirements for mobile operators are also being reviewed in a majority of member states. The report stresses the importance of ensuring that these requirementsare strengthened, that they follow the latest state-of-the-art practices and that their implementation by operators is effectively audited and enforced.

In its Conclusions[7] of 9 June 2020, the Council "recognises that increased connectivity, while empowering digital services, can result in citizens, companies and governments being exposed to cyber threats and crimes that are increasing in number and sophistication". In this context, it "emphasises the importance of safeguarding the integrity, security and resilience of critical infrastructures, electronic communications networks, services and terminal equipment" and "supports the need to ensure and implement a coordinated approach to mitigate the main risks, such as the ongoing joint work based on the EU Toolbox on 5G cybersecurity and the secure 5G deployment in the EU."

1. COM(2016) 588 of 14 June, 2016 on 5G for Europe: An Action Plan.

2. Commission Recommendation of 26 March 2019 on Cybersecurity of 5G networks C(2019) 2335 final.

3. EU coordinated risk assessment of the cybersecurity of 5G networks, NIS Cooperation Group, October 2019.

4. Cybersecurity of 5G networks EU Toolbox of risk mitigating measures, NIS Cooperation Group, January 2020.

5. COM(2020) 50 final of 29 January, 2020 on Secure 5G deployment in the EU -Implementing the EU toolbox.

6. Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity , NIS Cooperation group, July 2020.

7. Council Conclusions on Shaping Europe's Digital Future, 9 June 2020.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

September 2020

The "UK Turn" on 5G, a Domino Effect?

Esther Naylor
Chatham House

The UK has taken an intelligence-led approach in assessing the security of its critical network[1]. This model carefully balances the commercial imperatives of network providers with national security risk in the supply chain. An approach taken well before the current debate on 5G. Until July 2020 this method justified the national security risk posed by Huawei's involvement in the infrastructure through a separation of the 'core' sensitive parts of the network from its 'edge'/periphery. In an apparent U-turn however, the UK government has recently taken decisive action on the potential threat to the stability of its Critical National Infrastructure (CNI) by excluding Huawei from its network. The decision was taken amidst pressure from its closest ally – the US and rising global tensions with a powerful technological adversary – China.

ABANDONING THE STATUS QUO

In 2007, Huawei's equipment started being rolled out in the UK networks as part of a major infrastructure upgrade. In 2010, the

Esther Naylor, Research Assistant at the International Security Programme of Chatham House.

UK government established the Huawei Cybersecurity Evaluation Centre with the mandate of analysing Huawei's equipment for potential vulnerabilities with the aim of increasing the secure design of networks. When it came to the 5th generation of mobile networks, the UK continued, with a decision issued in January 2020, with its cautious approach allowing Huawei in a maximum of 35% of its kit in the network›s periphery. However, fast forward to July 2020, the UK government issued definitive guidance which significantly altered its approach stating that no new Huawei 5G technologies can be acquired after the end of 2020, and all existing Huawei equipment is to be stripped from existing infrastructure by 2027.

This U-turn was largely driven by the US issued sanctions, in May 2020, on semi-conductor chips which aimed to curb Huawei's efforts to 'undermine US export controls. In reality these sanctions restrict Huawei's ability to use US technology and software in designing its semiconductors, therefore disrupting Huawei's supply chain. Based on this decision, the National Cyber Security Centre (NCSC) issued a guidance stating that the UK could no longer manage the risk posed by using the company's technology in future 5G networks.

The U-turn caused an initial stir amongst the UK telecommunication providers whose arguments focused on the laborious, lengthy and expensive endeavour to remove existing Huawei's equipment from their network. However, the leaders of BT Group and Vodafone have acknowledged that since the 35% cap was imposed, they were already making such preparations, and they welcomed calls to diversify the supply chain[2].

Removing the equipment is only one part of the problem, the bigger challenge is finding suitable alternatives. Not only do these alternative 5G providers have to produce rival which is technically as good, if not better, they also are under a renewed obligation to enhance the security. 5G providers are under a spotlight. Security is built upon trust and strengthened through accountability and transparency. If there is distrust in one part of the network, the rest of the infrastructure could potentially be weakened and jeopardized.

LAYING THE GROUNDWORK FOR THE TURN ON HUAWEI

Serious cybersecurity concerns have been raised and tolerated throughout the UK's continued assessment of supply chain security,[3] and yet, the UK's decision on 5G demonstrated a significant U-turn by the UK government. This begs the question of whether it will stimulate a domino effect on other countries who are in the process of making similar decisions.

Countries who had already taken steps to limit Huawei 5G technology in advance of the UK's decision citing national security concerns include Australia, New Zealand, Japan, Taiwan and the US. Hence, the UK's decision aligns with that of its intelligence allies.[4] Nonetheless, many countries using Huawei technology already, in South East Asia, South America and Africa have expressed no

intention to follow suit.

As a further step, the UK has proposed a new coalition of likeminded states to counter the role of Huawei through a group named the D10. This group includes the G7: UK, US, Italy, Germany, France, Japan and Canada – as well as Australia, South Korea and India. The purpose of which is to explore and invest in alternative 5G suppliers. Scepticism surrounding this proposal raises the question of whether the venture can successfully meet its objectives and take into account the challenges of free trade and global markets.

The European Commission has also urged member countries to diversify 5G suppliers. EU member states enjoy the prerogative to decide on limiting or precluding the company from their national infrastructure. France has encouraged telecom providers not to switch to Huawei but has not required companies to discontinue using its technology. Given ongoing geopolitical tensions it is highly unlikely that the EU member states will follow the UK's example on its own accord. EU countries do not want their hand forced in the drawing of a digital iron curtain. It remains to be seen if 5G network technology provided by the 'made in EU' Nokia and Ericsson can rival the cost-effectiveness of Huawei and, if so, when. All eyes are on Germany to make a definitive decision on Huawei, which is expected soon. As is the case with several other countries, it will have to delicately balance its relationship with China and the demands of its telecoms industry.

A SECURE CYBER INFRASTRUCTURE

The dawn of the 5G revolution has forced governments to reconsider what is critical national infrastructure and what are the best ways to protect it. It forces imperatives upon countries to take greater steps to secure this infrastructure however expensive.

1. See recommendations from the Intelligence and Security Committee Report 2013 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/205680/ISC-Report-Foreign-Investment-in-the-Critical-National-Infrastructure.pdf and Huawei Cyber Security Evaluation Centre Report 2013 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/266487/HCSEC_Review_Executive_Summary_FINAL.PDF

2. Oral evidence given in a UK Defence Subcommittee on 5G https://committees.parliament.uk/oralevidence/782/pdf/

3. This caution was the product of various reviews and reports including: UK Intelligence and Security Committee, Statement on 5G Suppliers https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20190719_ISC_Statement_5GSuppliers_Web.pdf?attachauth=ANoY7cqHGcdVESj84FfMtqjpWpLYwHc8yD8fATQrlKU-l5Ibb_DOa61DRKcQQXkGCWLFs-Qk3zPnbqljRYee0fz4XKuKn2RNOJztn12MMJicfKvB5DJEdCwmzW8hXXmlxa8SQLhXfPZ6uBsb6p867DsQXJdUbNBMgUPN8URuFfBsQfEd-cQ5p6okC-D1MA-TBmu_MmZlzbhCymsw374MbgNAHYZLO

CHZFYMu5DnI-2d1P7yKjWT20Gw6A8hOKTQBrq-9Xz5QK7pd&attredirects=0, UK Department of Digital, Media, Culture and Sport (DCMS), UK Telecoms Supply Chain Review https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf, Huawei Cyber Security Centre Evaluation Report 2019 https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019

4. Note, the only member of the partnership who has not formally banned the company from its networks is Canada. https://www.reuters.com/article/us-canada-huawei-analysis/canada-has-eff...

The Race of Chinese Companies in the 5G Competition

Lyu Jinghua
Carnegie Endowment for International Peace

With the potential of enabling not only significant economic growth but also the innovation of critical technologies in various fields, both the US and China view 5G as one of the key influencing factors in the "great power competition". While the US believes that "the race to 5G is a race America must win", China views it as representing the major leapfrog of its position in ICTs by describing the progress as "1G behind, 2G follow, 3G breakthrough, 4G synchronization, 5G leading". Differently from competition in other traditional areas, companies rather than governments – the Chinese company Huawei as the most noticeable one – have played a significant role and become the pawns of the geopolitical game. Despite the obvious benefits such as lower costs and higher efficiency in using Huawei's products, the company is now under huge pressure of being excluded from 5G networks by more and more Western economies – especially following Britain's reversal of its decision.

Lyu Jinghua, visiting scholar with Carnegie's Cyber Policy Initiative. Her research focuses primarily on cybersecurity and China-U.S. defense relations.

All the declared concerns supporting the ban of Huawei, including the risks of surveillance and data collection and the potential vulnerabilities to cyberattacks or installed kill switches, sound reasonable at first. However, it is fair to say that these are inherent risks embedded in all ICT products. Why is Huawei so alarming, then? The frequently heard answer is that Huawei has much closer relations with the Chinse government than the usual ones, with three main accusations. Are they convincing enough?

The first and most primary accusation is that Huawei is forced to obey the laws, such as the National Intelligence Law and Cybersecurity Law, to transmit data to the government. There indeed are regulations about the obligation of cooperation and assistance for national security reasons, but according to a leading Chinese professor in cybersecurity law, Shenkuo Wu, the interpretation of how it affects Huawei's overseas operations is not accurate. It is stipulated that such obligations should only be fulfilled by the ICT companies directly operating within Chinese territory rather than their overseas subsidiaries. The latter, on the other hand, are clearly required by The Code of Conduct for Overseas Investment and Operation of Private Enterprises to comply with the laws and regulations of the host countries (regions). Clifford Chance, a global law firm headquartered in London, also concluded that «nowhere does Chinese law give Beijing the authority to compel telecommunication equipment firms to install backdoors or listening devices—or to engage in any behavior that might compromise network security."

The second argument is that the Chinese government has given Huawei as much as $75 billion in subsidies, which gives it incomparable advantages in the 5G market. It is a common practice for companies to receive government grants supporting high tech research and development. Moreover, audited data shows that in the 10 years from 2009 to 2018, the total amount of direct grants Huawei received from the Chinese government – mostly in R&D incentives – was just 0.3% of Huawei's total sales of $514 billion over the same period. The high volume of investment by Huawei in R&D, which was $15 billion in 2018 as shown by The 2018 EU Industrial R&D Investment Scoreboard, apparently contributed more to its success. Huawei is listed as the 5th among 50 companies in this report, while its main competitors such as Cisco, Nokia, and Ericsson are respectively listed as the 25th, 27th, and 43rd.

The third one suggests Huawei's close connection with the government because of the military background of its founder, Ren Zhengfei, and some other employees. It is well known that China has the largest amount of military personnel. The active force is currently 2 million, 2.3 million in late 2015, and even larger before. A report from PLA Daily shows there were altogether 5.7 million retired military personnel as of July 2018. Most of them retired at an early age and sought a second career as civilians. It is also very common for companies around the world to hire retired military personnel, but there is little suspicion of them working for the government behind the scenes.

From the perspective of most Chinese, the above facts highlighted the possibility that Chinese nationality is now the original sin of a company due to heightened geopolitical tensions. Its results will spill over far beyond one company, one industry, or one country. First of all, if commerce decisions are driven by non-market forces, then other Chinese companies with overseas business will question the significance of respecting the principles of free trade and abiding by international rules. Secondly, with Chinese companies being more inward-looking as the result of observing what Huawei and other companies such as TikTok have gone through, there will be fewer domestic markets for foreign companies and less investment from China in foreign markets, which will lead to economic losses for both sides. Third, if other countries show the willingness to choose sides between the big powers in the competition for 5G and then in other areas, the potential trend towards an undesirable high-tech cold war will be assured and soon come true. Is anyone winning in a geopolitical-driven 5G race where companies are the pawns?

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

September 2020

Will 5G Push Internet Voting?

Samuele Dominioni
ISPI

In the last months a meme went viral on social media networks that showed a multiple-choice test with the questions "Who is pushing remote working in your company?" the answers were "CEO", "CTO", "Covid-19". Mutatis mutandis this joke can be translated to many other sectors that are deeply affected by the pandemic. One of these is elections and voting modalities. Although it is not a brand new topic in the media, the urgency to make democracy work in pandemic time ignited a recent debate. Simultaneously, many governments are making decisions on 5G, which is "one of the most important innovations of our time".[1] Beyond the open confrontation between the United States and China, discussions were further fostered by the UK's decision to ban Chinese 5G technologies from its networks. This decision has been particularly under the spotlight as the UK did not ban Chinese technology in the first place. Thus, it fuelled the fire about the security and safety of critical infrastructures, including elections.

Samuele Dominioni, Research Fellow at the ISPI Centre on Cybersecurity, in partnership with Leonardo.

The pandemic triggered the necessity to find alternative solutions to in-person voting. Currently, the United States, as long as the postal service is put in the condition to work, is making it easier for citizens to vote absentee by mail to avoid postponing presidential elections. As a matter of fact, this has been the case in many other countries. In the last months just among Council of Europe member states, 12 elections have been postponed (including one presidential and two parliamentary). Despite concerns over election delays, one potential solution, internet voting, continues to be called into question, as many experts worry that they are not yet safe, especially for general elections. Indeed there are just a few countries (for example, Estonia and Switzerland) that have already implemented internet voting solutions.

Internet voting is just the tip of the iceberg of the use of digital tools in elections. We should consider elections as a cycle, composed of pre and post-election periods. This approach envisions elections as continuous processes rather than isolated events. As such, elections are considered not only in terms of election-day but integrated building blocks that include procurements, voters registration, result tabulation, etc. For some of these building blocks, electoral authorities use some degree of digital technology to improve electoral processes (such as office tools, websites, databases, voting technologies). The growing threats to the digital side of elections were the drivers that let the United States declaring elections as "critical infrastructure" in 2017. Therefore, even if we consider voting modalities or the electoral cycle as a whole, the digital dimension is an important variable to consider for the election›s integrity. So, how might the advent of 5G impact this element?

The fifth generation of mobile telecommunications could generate two main effects when it comes to electoral processes. The first one regards the opportunities; the second refers to the public perception of it. Speaking of opportunities: 5G technologies are safer than those developed so far. Indeed, 5G permits the encryption of more data, it is more software and cloud-based than previous systems (allowing for better monitoring), and it allows "network slicing" (which refers to the ability to segment the system into numerous networks that can be customized separately in terms of cybersecurity).[2] These characteristics could give further impetus to those who advocate for digital voting. For example, "network slicing" could be extremely relevant for building up cyber-secured voting networks. Moreover, as argued in one of our previous publications, due to the software nature of 5G, "the outlook for a future that relies on this technology and other new digital pathways is cyber-defined". In this sense, given the fact that 5G is mostly privately developed, "[C]ompanies must recognize and be held responsible for a new cyber duty of care", and "[g]overnment must establish a new cyber regulatory paradigm to reflect these new realities". Achieving these conditions could be a practical step towards increasing the cybersecurity of the election as critical infrastructure even within the context of 5G. So, would this technology eventually push for the concretisation of internet voting?

It may not be sufficient to push forward the idea of Internet voting among the population. Trust is still a huge issue when it comes to digital technologies. There are still large segments of the population that do not understand and thus do not trust digital technologies. For example, a recent Eurobarometer survey on cybersecurity showed that "[t]he majority of respondents (52%) feel that they are not able to protect themselves sufficiently against cybercrime" or that they are afraid of identity theft (66%). Trust is also a crucial issue concerning electoral integrity. Indeed, to accept the result of an election, electoral stakeholders (including voters) must trust the system. As reported in a recent analysis by the International Foundation for Electoral Studies (IFES), "the technology that underpins internet voting is highly sophisticated [...] most voters will not understand how it works, and this lack of understanding could undermine public trust".[3]

The advent of 5G would probably slightly increase distrust in digital elections (regardless of internet voting) for at least the following three reasons: first of all, as it was mentioned, it is a much more complex technology, which could lead to greater miscomprehension on how it works even among politicians and decision-makers. Second, the ongoing struggle between some western governments and some Chinese companies could weaken the perception of the neutrality and integrity of this technology as a whole. The accusations regarding possible spying activities through the 5G could, in turn, spark concerns among electoral stakeholders (raising issues such as endangering the sacred principle of voter secrecy). Finally, 5G is fuelling multiple conspiracies theories, which are spreading all over the world. Although deceptive tales frequently target information and communication technologies, these skyrocketed since the outbreak of Covid-19, fuelled by growing disinformation and the fake news phenomenon.

Therefore, even if we are living in a world that is in real need of new ways to vote remotely, the advent of 5G may generate contrasting effects. On one side, 5G technologies could help to enhance cybersecurity concerns regarding Internet voting. On the other, 5G could increase public distrust of Internet voting and thus on electoral integrity. The solution to this stalemate must be addressed with a comprehensive and consistent cybersecurity strategy vis à vis 5G technologies and with proper communication and dissemination campaigns for the general public and keep on fostering basic digital knowledge to the marginalized segments of the society.

1. Enisa, "Threat Landscape for 5g Networks", November 2019.

2. Lily Hai Newmann, "5G Is More Secure Than 4G and 3G—Except When It's Not", Wired, 15 December 2019.

3. Applegate M., Chanussot T., and Basysty V., "Considerations on Internet Voting: An Overview for Electoral Decision-Makers", IFES, April 2020.

ISPI
ITALIAN INSTITUTE
FOR INTERNATIONAL
POLITICAL STUDIES

September 2020

Italy, National Security, and 5G

Stefano Mele
Carnelutti

5G networks represent one of the key elements upon which the future process of digital transformation of both the economic and social level of each nation is based. Indeed, the potentialities of these networks will go well beyond the supply of telecommunications services between users. Accordingly, it will allow a more efficient and dynamic allocation of those related to other strategic and sensitive State's sectors, whether public or private, such as the financial and banking ones, energy, public health, transport, or those related to digital infrastructure, supply chains and so on.

Consequently, the security of 5G networks', as well as their capability to constantly guarantee the use of essential services by citizens, will be not just the main economic driver of the near future, but above all a fundamental element for countries' national security, including Italy.

In this context, although the Italian government has not yet tackled the issue of 5G networks' security in a strategic way, it can be still

Stefano Mele, partner in CARNELUTTI Law Firm, where he leads the Technology, Privacy, Cybersecurity and Intelligence Law Department. He is also the President of the Information and Communication Technologies Authority ("ICT Authority") of the Republic of San Marino

highlighted how the new regulation on the 'National Cybersecurity Perimeter' and the novelties brought to the discipline on the so-called 'Golden Power', will also have a positive impact on this sector.

Particularly, through the provisions of the 'National Cybersecurity Perimeter', the Italian legislator aims to ensure a high level of security of the networks, information systems and IT services of public administrations, of private and public entities and operators that have an office within the national territory, on which the exercise of an essential State function depends, or the supply of essential services in order to maintain civil, social or economic activities that are fundamental to the State's interests and from whose malfunctioning or interruption, even partial, or improper use, may derive a prejudice to the national security.

This goal – which is both essential as well as ambitious – will also impact the security of 5G networks. This will be achieved, on the one hand, by imposing the obligation to all private and public operators included within the 'National Cybersecurity Perimeter', to adopt the security measures developed, depending on their respective area of competence, by the Presidency of the Council of Ministers or by the Ministry of Economic Development, on the other hand through the verification activities of the National Evaluation and Certification Center (Centro di Valutazione e Certificazione Nazionale – CVCN). Indeed, this body, along with other various tasks assigned by the provision, will also have to carry out an activity of risk assessment, verification of the security conditions and absence of known computer vulnerabilities, whenever a public or private operator decides to provide for the supply of goods, systems and ICT services, that will be used on networks, informational systems and for the performance of computer services covered by the 'National Cybersecurity Perimeter'.

At the same time, the recent changes to the so-called 'Golden Power' will also indirectly have a significant impact on the security of 5G networks. As it is well known, this regulation guarantees to the government the possibility to exercise – in some sectors considered strategic and of national interest – the power of veto on the adoption of corporate resolutions or the purchase of shareholdings, as well as to impose specific requirements or conditions on each contract or agreement from which a serious prejudice to public interests may arise.

The latest updates of this legislation have subjected to the power of veto and to the power of imposing specific requirements and conditions also to the conclusion of contracts or agreements concerning the purchase of goods or services related to the design, construction, maintenance and management of the networks linked to the electronic telecommunications services with 5G broadband technology, or concerning the acquisition, for any reason, of technology-intensive components functional to the above-mentioned implementation or management, when realized with parties outside the European Union. To this end, the discipline further specifies that the elements indicating the presence of vulnerabilities, that

could compromise the integrity and security of the networks and data passing through them, including those identified on the basis of principles and guidelines developed at international level and by the European Union, are also subjected to an assessment.

Therefore, it is evident that, even in the absence of a specific strategy for the security of 5G networks, through the joint use of the 'Golden Power' and of the activities of the CVCN, the Italian government is concerned to regulate the urgency of a careful selection of suppliers of goods and services for the design, construction, maintenance and management of the 5G networks, even in the acquisition phase, for any reason, of the technology-intensive components functional to these activities. Furthermore, thanks to the 'National Cybersecurity Perimeter', the government aims to ensure a high level of security of these networks, as well as of the informational systems and services linked to them.

Italy, therefore, applies, as the central point of its security system, the criterion of careful selection of suppliers, avoiding the idea of using an approach based on a geographical origin parameter, as for instance, the United States, Australia or India have done with the technology of Chinese companies. Nevertheless, in order to obtain a similar result to that of these actors, not being able to exclude tout court non-European companies from the national market through a mere political decision, the Italian government has chosen to use the only effective possible approach, as to provide on the legal level that national companies who want to use the 5G technologies of non-European suppliers considered unsafe must be subjected to a series of strict requirements for their use, which go so far as to obtain from the supplier the possibility to carry out, even through third parties, processes of verification and control of the source code and hardware designs of the equipment. National companies will need to be able to prove these informations to the government upon request.

In conclusion, although Italy has so far arranged useful tools, a strategic and broader approach to support the security of future 5G networks still seems to be missing. In this sense, even just fully implementing, as quickly as possible, what has been recently provided by the European Union within its "Toolbox on 5G Cybersecurity", would represent a decisive step forward among what can already be defined as the single most important global man-made critical infrastructure of the past thirty years.