Études de l'Ifri

WHAT IS DIGITAL POWER?

Jean-Christophe NOËL

November 2019

French Institute
of International
Relations

The **French Institute of International Relations** (Ifri) is a research center and a forum for debate on major international political and economic issues. Headed by Thierry de Montbrial since its founding in 1979, Ifri is a non-governmental, non-profit organization. As an independent think tank, Ifri sets its own research agenda, publishing its findings regularly for a global audience. Taking an interdisciplinary approach, Ifri brings together political and economic decision-makers, researchers and internationally renowned experts to animate its debate and research activities.

A global leader in consulting, technology services and digital transformation, **Capgemini** is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of over 200,000 team members in more than 40 countries. The Group reported 2018 global revenues of EUR 13.2 billion.

This study has been carried out within the partnership between Capgemini and the French Institute of International Relations (Ifri).

Capgemini

ISBN: 979-10-373-0092-8

The opinions expressed in this text are the responsibility of the author alone.

How to cite this publication:
Jean-Christophe Noël, "What is Digital Power?",
Études de l'Ifri, Ifri, November 2019.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tel.: +33 (0)1 40 61 60 00 – Fax: +33 (0)1 40 61 60 60

Email: accueil@ifri.org

Website: Ifri.org

Author

Jean-Christophe Noël is an Associated Research Fellow at Ifri's Security Studies Center.

He is a former French Air Force officer. After pursuing a career as a fighter pilot, he held various staff positions, dealing in particular with doctrinal or prospective matters. He was also the Deputy Chief of Staff of the French Air Force Chief of Staff from 2006 to 2009, a Military Fellow at the Center for Strategic and International Studies in 2009-2010 in Washington DC, and was in charge of politico-military affairs at the Policy Planning Staff of the Ministry of Foreign Affairs from 2012 to 2017. He currently teaches at Sciences Po Paris.

Jean-Christophe Noël graduated from the French Air Force Academy, Sciences Po Paris and the French *École de Guerre*.

Summary

Digital power refers to any actor’s ability to exploit digital data to help influence the behavior of other actors on the international stage and to achieve its own ends. It is about understanding how it influences events in the real world, despite its “intangible” nature.

It extends beyond the network where connectivity and flow are valued. Hence, digital power goes beyond the mere conventional state framework and reconfigures the standard categories, since all connected actors are theoretically likely to have a part in it.

It can be exercised for the benefit of conventional activities, but new practices of domination have been imposed on it. The target itself provides the conditions for its control, by asymmetrically revealing its characteristics. This information is transformed into knowledge and power provided it can be processed and enriched. The algorithmic or psychological structure of the target becomes transparent. The exercise of digital power is less an attempt at coercion or seduction than at subjection.

Being powerful in the digital world requires the ability to create a favorable ecosystem, to control data, to control networks’ competitive edges and to coordinate its digital capacities with other forms of power. Nevertheless, the exercise of digital power could deteriorate over time, with increasing influence of the real world on the digital world. States are testing many strategies to weaken the hyperconcentration of power of some actors and rebalance the distribution of wealth and power.

Finally, digital power is a complex and multi-faceted subject. It is a power both conventional and network-based, liberating and controlling, shared and fragmented, asymmetrical and contained, fragile and transient, but that can bypass obstacles. It is continuing to evolve as people invent new practices. Finally, it is like a kaleidoscope, with several aspects whose coordination sometimes generates considerable tension.

Table of Contents

Introduction

What is meant by digital?

Digital data can be recorded, stored, compressed or transferred without any loss of information and quality. The enhancement of these characteristics has been essential for the development of computing, to the point that the term digital has entered into everyday language to generically refer to computer science applications.[1] The development of ever more sophisticated algorithms, combining this data through calculation, makes it easier to solve problems previously considered as too complex. The continuously improving power of microprocessors is reducing calculation times. The implementation of common protocols to easily exchange data between computers is redefining the concept of connectivity between people. Information, commands and stimuli are circulating in ever greater numbers and dramatically changing how complex systems interact and operate.

Digital technology: a political issue

Therefore, the trend of long-distance communication, which started with writing and continued with the printing press, telegraph, telephone and radio, carries on.

The digital revolution is dramatically changing large areas of human activity. It is shaping globalization by changing the distances between people. Transport, logistics, energy distribution, international finance and critical infrastructure management systems could not function without its applications. The volume of email exchanges is also impressive: 44.7 billion SMS and MMS messages were sent in France in the first quarter of 2018.[2] As of 12 August 2019, more than 45,584 billion emails had been shared worldwide since the beginning of the year.[3]

In the military field, the most advanced armies have integrated battlefield digitalization into their thinking. Military headquarters operate in a more decentralized way, taking advantage of the resources provided by

[1] D. Cardon, *Culture numérique*, Paris: Presses de Sciences Po, p. 18.

[2] “Le nombre de SMS envoyés en France”, *journaldunet.com*, 8 May 2018.

[3] “Emails envoyés dans le monde”, *planetscope.com*, accessed on 12 August 2019.

computerization, materializing the advent of a "revolution in military matters".[4]

From a cultural point of view, games are played on a network. The most talented players earn their living by participating in media tournaments. Special effects are pervading cinema screens, bringing artificial universes to life. A digital culture is emerging.

Digital technology is at the heart of economic, military and cultural issues. It has entered into the everyday life of all people connected to the Internet worldwide. It provides resources in terms of wealth, power, control of society and privacy. For example, Denmark, which is aware of these issues, appointed a Tech Ambassador in 2017. It is legitimate to talk about digital power.

What is power?

Defining the concept of power is a challenge. Common sense accepts that "power" on the international stage is the equivalent of "authority" within societies. However, such an understanding is of limited use. The national and international stages operate under different rules. Authors seeking to understand it acknowledge that it is one of the most controversial terms in international relations.[5]

However, two major themes regularly recur in discussions. The first attempts to make this concept operative. If power exists, it must be possible to define its components and assess them, to measure them in order to act rationally. In this context, power has long been reduced by the realist school to geographical location and to the sum of military, demographic or economic resources. The most intangible components, such as national pride, the quality of staff and policy, could also count. This accountable and analytical approach, however, is criticized insofar as it only reveals the potential of power. If a state actor does not combine them effectively, it does not guarantee any results. The Soviet Union had many of these advantages, but collapsed without fighting.

Another theme often recurs in discussions on the nature of power. Power is what decides the outcome of the interaction between two state entities or actors in the international system. It no longer refers to a

[4] A. F. Krepenevich, "Cavalry to Computer: The Pattern of Military Revolutions", *The National Interest*, No. 37, Autumn 1994, pp. 30-42; E. A. Cohen, "A Revolution in Warfare", *Foreign Affairs*, March-April 1996, pp. 37-54; J.-C. Noël, "Intelligence artificielle : vers une nouvelle révolution militaire ?", *Focus stratégique*, No. 84, Ifri, October 2018.

[5] R. Gilpin, *War and Change in World Politics*, New York: Cambridge University Press, 1981, p. 18.

potential, but “to taking action”.[6] In a seminal article, Robert Dahl defines it as: “A has power over B to the extent that A can get B to do something that B would not have otherwise done”.[7] Power restricts, but not necessarily in a violent way. It can be exercised through seduction, rather than by the brute imposition of will.[8] Finally, power corresponds to an actor’s ability to change the behavior of other actors on the international stage in a favorable direction.

What is digital power?

How can we describe digital power, sometimes called cyberpower, in this context? We will consider digital power as any actor’s ability to exploit digital data to help change the behavior of other actors on the international stage and to achieve its own ends.

It extends beyond the conventional state framework and reconfigures the standard categories, since all connected actors are theoretically likely to have a part in it. Furthermore, the sources of digital power lie in the exploitation of a synthetic environment and data. This study aims to understand how “intangible” power manages to influence events in the real world and to describe its potential, its applications, and its restrictions.

Digital power transforms the real world through enhancing cyberspace’s network properties (1) and new practices of domination that are imposed on it (2). Its components can be deduced from this (3). However, it is likely that its exercise will be changed in the future through a more assertive, proactive approach by actors in the real world (4). Finally, it is like a kaleidoscope, with several aspects whose coordination sometimes generates considerable tension.

[6] T. de Montbrial, “Qu’est-ce qu’une puissance au XXIe siècle?”, Speech at the Academy of Moral and Political Sciences, 7 January 2013.

[7] R. A. Dahl, “The Concept of Power”, *Behavioral Science*, 1957, No. 2, pp. 201-215.

[8] J. Nye, *Soft Power*, New York: PublicAffairs, 2005.

How the virtual world influences the real world

Power and the network

In 2016, Jelle van Haster defined cyberpower as "the variety of powers that circulate in cyberspace and which shape the experiences of those who act in and through cyberspace".[9] According to this Dutch expert, digital power is closely linked to cyberspace, the environment that it emerges from, and is deployed and used in.

Indeed, discussing digital power through cyberspace seems to be a relevant approach to better defining its boundaries. However, defining cyberspace is once again a challenge, as there are conflicting ideas. It is alternatively depicted as an area, a theater of operations, an environment, a space, a substrate, a medium, or a means.[10] This abundance of definitions does not just reflect a simple academic debate between exacting universities. Innovative strategic thinking underpins these different points of view. So, Moscow does not consider cyberspace as a unique place with its own specific features that impose particular rules and behavior. For the Russians, digital technology is like any other media that is involved in the control of information.[11] It fulfills a sovereign function more than it occupies a space.

Whether it is considered as a medium[12] or as an environment,[13] cyberspace more or less comes down to intranets and the Internet. Its

[9] J. van Haster, "Assessing Cyber Power" *in* N. Pissandis, H. Rölgas and M. Veenendaal, *8th International Conference on Cyber Conflict*, Tallinn: NATO CCD COE Publications, 2016, p. 13.

[10] A. Desforges, "Les représentations du cyberespace: un outil géopolitique", *Hérodote*, No. 152-153, 2014, p. 67.

[11] K. Limonier, "La Russie dans le cyberespace : représentations et enjeux", *Hérodote*, No. 152-153, 2014, p. 143.

[12] According to P. Cornish, cyberspace is a "global medium for communication and information exchange between computers and their human operators, an environment (of sorts) in which it is possible that digital signals are sent, received and processed." See P. Cornish, "Governing Cyberspace through Constructive Ambiguity", *Survival*, Vol. 57, No. 3, 2015, p. 153.

[13] For W. H. Boothby, cyberspace is "the environment formed by physical and nonphysical components characterized by the use of computers and the electromagnetic spectrum to store, modify and exchange data using computer networks." See W. H. Boothby, *Conflict Law: The Influence of New Weapons Technology, Human Rights and Emerging Actors*, Hague: TMC Asser Press, 2014, p. 123.

organization is that of a decentralized network, which has no center and borders, but where some nodes are more valuable than others.[14]

The power provided by a network differs significantly from conventional power, which is often condensed to a simple balance of power. The network values the link, the flow, and the mobility of items compared to the place, location and rootedness. Entering into and becoming part of a network is an immersive and encompassing experience. Anybody immersed in a network becomes a network; the connected object or person acquires the network's power, and a slow network will always be swallowed up by a more agile (or quicker or more efficient) network.[15]

Therefore, digital power must first be understood and studied as a phenomenon exercised through a network. Yet, network power was already the basis of some states' dominance.

Naval power

Naval power is a fine example of this, with the Athenians, Carthaginians and Etruscans during Antiquity and the Genoese and Venetians in the Middle Ages, and the defining of the first boundaries in the Mediterranean. But their influence was mainly commercial and prevailed along coasts. It was the emergence of the British Empire from the 16th century, in competition with the United Provinces,[16] that brought this concept to maturity.

Whereas the Spanish and Portuguese considered the New World as a reserve to plunder, the British set out to conquer the voids in order to develop them and impose their political system. Control of the oceans should make it possible to establish dominance through trade and commerce, the spread of liberal ideology and utilitarianism. Control of the lines of communication and of distances accelerated the growth in flows of goods, soldiers and ideas between the ports held by the British. London was the center of the network, and maritime bases formed the different nodes in the network that were equally entry points to uncharted territory. British naval power was primarily at the service of a political vision.

[14] P. Cardon, *Culture numérique, op. cit.*, p. 27-36.

[15] P. Bellanger, *La souveraineté numérique*, Paris: Stock, 2014, pp. 30-31. See also A.-M. Slaughter, *The Chessboard and the Web: Strategies of Connection in a Networked World*, New Haven: Yale University Press, 2017; D. S. Grewal, *Network Power: The Social Dynamics of Globalization*, New Haven: Yale University Press, 2008.

[16] C. Schmitt, *Le nomos de la terre*, Paris: Presses universitaires de France, 2001; P. Forget and G. Polycarpe, *Le réseau et l'infini*, Paris: Economica, 1997, pp. 53-77; F. Gipouloux, *La Méditerranée asiatique*, Paris: Presses du CNRS, 2009.

Scientific advances and the mathematical decryption of nature made this conquest possible. Their application in cartography and in astronomy provided the means to identify and sail across the vast expanses of oceans without getting lost. The world is described mathematically by a series of numbers called latitudes and longitudes, whose origin is obviously close to London, at Greenwich. It was deciphered. It could be used for moving and acting.

Actors of very diverse origins co-evolved in this environment. Soldiers, merchants, migrants and travelers rubbed shoulders with pirates, and even sometimes privateers, whose status blithely blurred the sovereign and criminal categories.

Digital power

While the sea is a natural environment, cyberspace was artificially created by humans. It is made up of three layers. The first is tangible (*hardware)* and includes all the physical infrastructure required to pass data from one network point to another. It specifically includes submarine cables, servers, computers and connected objects. The second layer is intangible and corresponds to the applications required to process information (*software*). It is made up of software and operating systems. The last layer is called the cognitive layer. It refers to the content of information stored and exchanged in the network.

Different laws or findings characterize the qualities of this network. According to Robert Metcalfe, the inventor of the Ethernet, "the value of a network is proportional to the square of the number of its users".[17] A network made of five computers has a value of 25. If you double the number of computers to come to 10, the value quadruples and reaches 100.[18] The entrepreneur, Gordon E. Moore, stated for his part that "at the same price, a microprocessor's computing power doubles every 18 months. Over the last 15 years, machines' computing power has been multiplied 1,000 times".[19] The German mathematician, Martin Grötschel, completed this empirical law and stated that, "the calculation speed of these machines, due to the growth in the efficiency of the algorithms, is progressing 43 times quicker than Moore's law".[20] The possibilities offered by cyberspace are increasing at an

[17] P. Bellanger, *La souveraineté numérique, op. cit.*, p.27.

[18] Qualifications have been made to this law. See B. Briscoe, A. Odlyzko and B. Tilly, "Metcalfe's Law Is Wrong", *spectrum.ieee.org*, 1st July 2006.

[19] P. Bellanger, *La souveraineté numérique, op. cit.*, p. 27. Between 1971 and 2001, the density of transistors doubled every 1.96 years.

[20] *Ibid*, p. 29.

exponential rate. Digital power is a liberating power that increases Internet users' capacity to act.

Cyberspace is not a fixed environment where the laws of physics closely support innovation. It is continuously evolving, mainly through the understanding and initiatives of individual and private actors who develop software that is released virally if it satisfies a need.[21] Digital applications are also made and dumped very quickly. Competition is fierce between entrepreneurs, as in China where, to paraphrase a famous proverb, "all is fair in war and.. between start-ups".[22] Advances in technology and market demand inspire each other and continually deliver new solutions. The 5G standard is just about to be implemented in the field of mobile telephony. However, yesterday's champions, like Ericsson, have fallen from their pedestals for failing to anticipate market developments. On the contrary, Huawei has managed to invest in projects that now give it an essential role in increasing its business opportunities. Digital power is exercised in a highly competitive environment of creative destruction, where innovation is generally bottom-up. It will be temporary if its owner does not have state-of-the-art technological tools.

As in the case of the sea, many actors with heterogeneous statuses have access to cyberspace. States, companies and individuals can interact among themselves, trying to achieve a wide variety of goals. This connection makes it possible to initiate more direct power relationships than previously, and to make genuine efforts to influence their contact or rival. Digital power is power, shared or even decentralized, between a variety of actors that operate in cyberspace.[23]

This phenomenon is accentuated by the fact that the Internet was originally designed according to a libertarian logic, guaranteeing that each connected individual would be offered a share of freedom and initiative by bypassing the monopoly of traditional institutions. Furthermore, cyberspace is not a *global commons*, a term that defines a space where no sovereignty is exercised, but whose use can benefit everyone.[24] Rather, it can be compared to a condominium where "a set of bits moving from one computer to another are usually on a network that someone owns and that is physically

[21] D. Cardon, *Culture numérique, op.cit.*, pp. 101-110.

[22] K.-F. Lee, *AI Super-powers: China, Silicon Valley and the New World Order*, New York: Houghton Mifflin Harcourt Publishing Company, 2018, pp. 40-50.

[23] T. Gomart, "Entre concentration et dispersion: le bel avenir de la puissance", *Politique étrangère*, Vol.84, No. 1, 2019, pp. 11-21.

[24] B. R. Posen, "The Command of Commons: The Military Foundation of U.S. Hegemony", *International Security*, Vol. 28, No. 1, 2003, p. 8.

located in a sovereign country".[25] Submarine cables that carry data through optical fibers may, for example, belong to private actors who have reserved use or rent a part of their capacities. They can also be co-owned by different actors in consortiums.[26] Therefore, states do not have the monopoly of these networks and cannot easily impose their rules.

The development that began on the oceans in the 16th century is still carrying on today. The algorithms are an extension of human beings and their brains in the digital world. They reflect people's choices, decisions, preferences and tastes in a different language. They digitally encode their behavior and turn people into a measurable quantity.[27] The discovery of the laws of physics and the translation of nature into mathematical language made possible the era of great discoveries and the conquest of the world by the Europeans; the partial digitalization of humans and the unmasking of their cognitive capacities could, in turn, cause major upheavals, carrying over from cyberspace to the real world.

Cyberspace is an environment where a new relationship between people and networks is being established. Control of the sea helped thalassocracies to emerge. Control of digital space could bring about the development of digitocracies. According to what practices, it remains to be seen.

[25] J. A. Lewis, "Cybersecurity: Next Steps to protect Critical Infrastructure", *Testimony to the US Senate Committee on Commerce, Science and Transportation*, 23 February 2010.

[26] Speech by Jean-Luc Vuillemin during a closed seminar at Ifri on 11 July 2019.

[27] P. Bellanger, *La souveraineté numérique, op. cit.*, p. 101.

Practices in cyberspace

The way in which digital resources are used in cyberspace is at the heart of the definition of digital power. A debate on this topic opposes those who consider that the exercise of cyberpower is only part of conventional forms of competition and those who assert that the nature of rivalry between states is, on the contrary, overthrown, and that new models should be favored.[28]

New technology at the service of conventional objectives

Since the beginning of the 1990s, cyberspace has been identified as a new theater of operation where violence will inevitably be unleashed.[29] However, nothing significant has happened. Analysis can be finetuned; in 2012, Thomas Rid explained in a seminal article that cyberwar never existed, that it does not exist, and that it is highly likely that it will not break out in the future.[30] The most publicized cyberattacks are only modernized and sophisticated versions of acts of subversion, espionage or sabotage. The states are just modifying the modalities of operations with the new resources at their disposal.

The fear that a gifted, evil young man might succeed in paralyzing security organizations from his basement appears closer to a fantasy than to an actual possibility. Admittedly, opportunities exist, and breaches in systems can be expanded to sometimes get some impressive results widely covered by the media, but that are very short-lived operationally. For example, a 20-year-old German man succeeded in publishing personal information about around 1,000 German politicians, including the Chancellor Angela Merkel, on the Internet. Without having great hacker skills, he managed to extract all the information about his victims available on the web, before compiling and spreading it.[31]

However, obtaining military results requires a substantial mobilization of resources, similar to preparing for a conventional military targeting operation.[32] A systemic analysis of the target must be carried out.

[28] W. Hoffman, “Is Cyber Strategy Possible?”, *The Washington Quaterly*, Vol. 42, No. 1, 2019, pp. 131-152.

[29] J. Arquila and D. Ronfeldt, “Cyberwar Is Coming!”, *Comparative Strategy*, Vol. 12, No. 2, pp. 141-165.

[30] T. Rid, “Cyberwar Will Not Take Place”, *Journal of Strategic Studies*, vol.35, no. 1, 2012, p.6.

[31] “Cyberattaque en Allemagne: le hacker vivait chez ses parents”, *latribune.fr*, 8 January 2019.

[32] Interview, 20 June 2019.

Its architecture and operation need to be perfectly known. Specific information must be obtained to discreetly penetrate the opponent's system. The preparation of the attack software must be sufficiently formulated to avoid collateral damage. However, failure is still possible. The simple changing of a password by an opponent's operator can ruin months of investigation.[33]

Attack software can only be used once. It is a one-strike weapon; it ceases to be operational as soon as the opponent understands that they have been deceived and corrects the faults in their shield.[34] Paralyzing a system is not always enough to achieve a lasting military result. Only the destruction of the target can be. As the strategist Colin Gray summarized it, the main added-value of cyberpower in the field of military confrontation is to be a catalyst, an *enabler* in joint operations.[35] *Orchard* is the name of Israel's 2007 operation over Syria to destroy a site under construction that was to host nuclear facilities. Israeli cyberoperators broke into the Syrian air detection system and masked the radar echoes of the *H'eil Ha'Avir* (Israeli Air Force) aircraft. Their contribution proved decisive in surprising the opponent and maintaining freedom to maneuver. Although cyberpower cannot solve military problems, it allows them to be tackled from a stronger position.

Finally, digital power does not seem to bring about disruption in the field of coercion.[36] Its use there is particularly sensitive, as the opponent may misperceive the attacker's intention. The attacker would first have to decide whether to inform their rival of their attack. If they do not do this, the latter could believe that they are the victim of a computer failure, or fear, to the contrary, that they are the target of a pre-emptive attack and react in an extreme way in the event of a serious crisis. However, if they choose to inform their opponent of their move, the latter will be able to analyze the attacker's mode of action and ward it off. Shows of strength and efficiency scarcely seem compatible.

Furthermore, the content of the message sent may be difficult for the defender to detect, if the extent of the damage exceeds the threshold that was originally intended, because of faulty programming by software. Control of the escalation can escape the attacker's control. The Stuxnet virus, intended to sabotage the Iranian nuclear program's uranium enrichment, spread to

[33] *Ibid.*

[34] However, these algorithms can serve as a "stem cell" and mutate if skilled hackers partly reconstruct them. They are then successfully reused.

[35] C. Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling*, Carlisle: Strategic Studies Institute/US Army War College Press, 2013.

[36] To qualify this point of view, see S. Taillat, "Dissuasion et coercition" *in* S. Taillat, A. Cattaruzza and D. Danet, *La cyberdéfense : politique de l'espace numérique*, Paris: Armand Colin, 2018, pp .147-148.

other computers worldwide.[37] If other highly sensitive functions are affected, the reaction can trigger a cycle of reprisals that is difficult to stop.

At first glance, cyberpower participates with its own characteristics in the exercise of conventional power. The advent of digital technology has not changed states' or even individuals' interests and motivations, which remain constant.[38] It mainly contributes to conventional forms of competition and confrontation. The challenge is to integrate it correctly with other tools of conventional power, such as military force.

The need to define new paradigms

Despite these restrictions, the frequency and volume of attacks are continually increasing in cyberspace. A total of more than 200 events that could be considered as cyberattacks by one state against another have been identified.[39] Criminal actions are also multiplying on the Internet. The number of harassments committed via an online communication service doubled in France between 2016 and 2018.[40] Although the characteristics of the digital network have already been mentioned, a description of the benefits of cyberspace is useful in understanding this increase in attacks and in better addressing digital power.

Principles of action in cyberspace

The spread of messages and data is first and foremost immediate and global in cyberspace. Any two computers can exchange information instantly provided that their communication protocols are compatible. Physical geography no longer counts. The scale effects are disproportionate with what was practiced beforehand. If an attack is possible, it can spread extensively and quickly. Military theaters of action acquire a global dimension. Although the physical operations are contained in the war zones during conflicts, sympathizers living in areas far removed from combat, or even in an enemy country, can also play a role. Conventional concepts of boundaries and sovereignty are being challenged.

Offensive means of action are favored. Access to the network is easy and requires modest investment. The cost/result ratio is particularly low and may encourage hackers to act. Failure will have little effect. The attacker also has the initiative. A computer system is similar to a fortress. It is fixed. It can

[37] "Stuxnet also Found at Industrial Plants in Germany", *h-online.com*, 17 September 2010.

[38] J. A. Lewis, "Étude préliminaire sur les analyses en cybersécurité ; l'affaire Snowden comme étude de cas", *Hérodote*, No. 152-153, 2014, p. 33.

[39] M. Willett, "Assessing CyberPower", *Survival*, Vol. 61, No. 1, p. 85.

[40] "L'état de la menace liée au numérique en 2019", *interieur.gouv.fr*, 9 July 2019.

be observed, its defenses can be tested, its faults detected and exploited. It is difficult for the defender to imagine all the possibilities for penetrating their network and to protect themselves against them. One of the hacker's favorite modes of action is to identify a weakness, known as "zero day", corresponding to a security fault in the software or the operating system that the designers are not aware of.[41] Imagination is the hacker's greatest strength.

The attacker also acts covertly. It is very difficult to immediately detect an attack and then to trace the intricacies of the network to identify the perpetrators. The initial priority is rather to understand the nature of the attack to limit its effects. The attribution phase only comes afterwards. And it is very unlikely to find a "smoking gun" identifying the origin of the attack with certainty. Various criteria have to be gathered and interpreted.[42] States can cover their tracks by entrusting the performance of some sensitive tasks to private actors. In any event, this stealth boosts the incentive for hackers to act, since they know they will have relative immunity.

Finally, common rules of engagement or a code of good practice shared by all do not exist in cyberspace. Actors' behavior can be very different and unpredictable because of a lack of regulation. Uncertainty and mistrust reign because actors ignore their rivals' capabilities and the limits they set themselves.

Therefore, digital power is also an asymmetrical power, reducing the power gap and capacity to act between the different actors.[43]

Digital power and business[44]

Private business entrepreneurs were the first to understand how to best possibly coordinate all these resources. They envisaged a new form of organization, overthrowing value chains and the dominance of established companies.

Start-ups are breaking free from the Taylorist model and promoting "scalability". Since they can theoretically reach all Internet users at very low financial cost, they are developing new products that they can continue to "manufacture" in the event of a growth shock, if demand rapidly explodes.

[41] J.-L. Gergorin and L. Isaac-Dognin, *Cyber. La guerre permanente*, Paris: Le Cerf, 2018, p. 109.

[42] *Ibid.*, p. 150.

[43] *Ibid.,* p. 157.

[44] N. Colin and H. Verdier, *L'âge de la multitude: entreprendre et gouverner après la révolution numérique*, Paris: Armand Colin, 2015.

Small teams with a great deal of autonomy have been established. Initially, for example, Wikipedia was grouped around eight people. Facebook had 450 employees in 2007 (as opposed to 35,000 in 2018).[45] Clients are responsible for voluntarily and freely supplying the components required for a start-up's development. An original idea is exploited by imagining a simple prototype. For example, the objective is to manufacture a luxury car, but only the engine is fitted on a chassis and four wheels. The rest is designed by the clients. Their preferences and wishes are known and applied through direct interaction with them. It is enough to offer them what suits them best. Entrepreneurs are taking advantage of the network's collective intelligence while individualizing the service. Supply and demand meet directly without intermediaries. Financial losses are sometimes high at the outset, but are largely offset by future profits. Growth is ensured by means of marketing technologies and addictive psychological skills. Faithfulness is rewarded by benefits and exclusive discounts.

Digital platforms obviously do not manufacture cars, but they do provide services. They aggregate them to make them even more attractive and to dominate the market. You are no longer selling a vehicle, but a life experience. You are no longer selling a hotel room, but a trip. Software is replacing intermediaries and transaction services. The digital platforms are responsible for finding the most attractive offers for potential tourists, saving them time and money. They combine offers from hotel groups with those of transport companies.

Besides controlling the value chain, these platforms are tempted to control digital infrastructure to manage data flows more closely. Controlling interfaces, like mobile telephones, is essential for clients to exclusively access the platforms' applications. Amazon started by selling books. The US firm then digitalized the content that was only readable on the *Kindle*. It now manufactures the chips that power these e-readers.

Clients are becoming captives of an ecosystem that is unevenly shared. The platforms are becoming indispensable by developing a world where the more or less artificial needs of its inhabitants are satisfied. In return, they collect an invisible tithe, made up of the data their clients will asymmetrically provide about their behavior and preferences. It is the source of the platforms' wealth that will make them grow. Advertising (Facebook and Twitter) is individualized. Of course, mapping services inform users of their locations, but they also provide them with several nearby addresses that are likely to trigger an irrepressible desire to consume.

[45] "Nombre d'employés de Facebook 2004-2018", *Statista.com*, accessed on 16 August 2019.

This tithe makes customers even more indebted since they become even more dependent on the services provided by the platform.

However, this data no longer belongs to them. It is in the hands of the large companies, which turn it into instruments of power. Data is not the new *oil* in business, but its new *soil*.[46] All the connected individuals are the new serfs of the digital era. They are tenant farmers who are cultivating, maintaining and developing the digital soil that does not belong to them and that they can suddenly be denied access to, if their masters so decide.[47]

The purpose of these platforms is to create a closed, hyperconcentrated system where they can eliminate any competition. They can then order the data according to their own logic, and influence many areas, such as work, privacy and taxation. For example, Facebook wants to issue its own money with Libra. They embody a modern version of the large colonial companies that took on commercial and then state and military roles, like the *East India Company* between the 17th and 19th century, that had India in its clutches.[48]

Between war and peace

Methods applied successfully in the economic field are gradually adopted in the field of conflict. Exercising digital power particularly appears to extend into the "gray area" that no longer corresponds to a state of peace, but cannot yet be considered as a state of war. The purpose is not to strike a decisive blow. The intention is rather to slowly penetrate the opponent's digital networks to become established there permanently and to exploit them if opportunities occur or circumstances dictate it. The sum of blows struck over all these networks must ultimately weaken the enemy.

Scalability and a change of scale make it possible to redefine the conflict conditions and to reconsider some categories of international competition. To paraphrase Valery Gerasimov, the role of non-military means to achieve political and strategic goals is increasing.[49] Sometimes, cyberactions prove more effective than armed force, blurring our societies' relationship to violence.

The level of conflict where digital power seems most decisive is that of "political warfare". This term dates from the beginning of the Cold War. George Kennan first defined it as the logical application of Clausewitz's

[46] L. Kirchner, "Data is the New Soil: David McCandless' TED talk on Visualizing Data", *Columbia Journalism Review*.

[47] Interview, 10 May 2019.

[48] J. Keay, *The Honourable Company: A History of the English East India Company*, London: HarperCollins, 1991.

[49] M. Galeotti, "The Gerasimov Doctrine and Russian Non-Linear War", *kcl.rl.talis.com*, 2013.

doctrine in peacetime, that is to say, the use of all means available to a nation, with the exception of war, to achieve its national goals.[50] A more recent definition interprets it as "the intentional use of one or more components of power (diplomatic, information, military and economic) to influence the political make-up or the decision-making process within a state".[51]

Digital power influences this political warfare. Tactical, operational or strategic levels are abandoned in relation to conventional conflict. It is no longer a question of succeeding on the conventional battlefield, of maneuvering better than opposing armies, or of destroying means of arms production and logistic support. The purpose is to bypass all these conventional levels of war and to directly target citizens, by acting on their perception of reality and guiding their political preferences.

Domestic political debates are formatted and the legitimacy of some leaders is weakened or boosted by using procedures similar to those of commercial marketing. The same psychological bias helps to attract and retain Internet users. Never mind the exact accounts of events. For example, false stories with an exciting narrative circulate six times quicker than real facts on the Internet. Virality is exceeding truth. The feeling of belonging to a group with similar ideas, feelings or values is also a powerful driver for bringing scattered individuals together under a common theme. The impression of being right is even stronger. The fact that people do not usually like being wrong, and hate it even more when a third party shows them their mistakes, highlights the difficulty in setting the record straight.[52]

"Monarchs" are emerging on the Internet, who know how to play on human psychology, seducing a vast audience and seizing debates for their benefit. The phenomenon of hyperconcentration at work in the growth of platforms is found here. A study of 330 million Chinese Weibo users showed that fewer than 200,000 members had more than 100,000 *followers*, and that only 3,000 of these were followed by more than a million individuals. Opinions are mainly formed from messages sent from only 300 accounts.[53]

These principles have been adopted in many ways by political entrepreneurs. The Five Star Movement in Italy expanded rapidly and took power thanks to G. Casaleggio, a real Internet marketing expert. He relied on the popular and friendly image of Beppe Grillo, an Italian comedian who

[50] L. Robinson, T. C. Helmus, R. S. Cohen, *et al.*, *Modern Political Warfare,* Santa Monica: Rand, 2018, p. XIII.

[51] *Ibid*, p. 7.

[52] *Ibid*, pp. 118-147 for this paragraph.

[53] P. W. Singer and E. T. Brooking, *Like War: The Weaponization of Social Media*, New York: Houghton Mifflin Harcourt Publishing Company, 2018, p. 130.

is critical of traditional political parties, by offering to write his blog posts. Within the space of two years, Beppe Grillo's blog became one of the top ten blogs in the world. Internet users' reactions were scrutinized and analyzed. The most "liked" topics were continued and developed. The aim was really to capture Internet users' attention and retain them by giving them what they wanted. The transition to the real world and political competition was achieved by sticking to the same principle. It was still necessary to recognize, develop and maintain people's beliefs, but also to provide a simple and consensual reason capable of explaining the cause of their frustrations. The explanation found in Italy was the failure of the elites. Although very brief, this narrative made it possible to unite various groups with very diverse, even contradictory, political opinions. Each one considered that their situation was the result of the country's disastrous management by politicians who were incompetent.[54]

Variations exist in this revamped form of propaganda. Moscow plays less on populism than it seeks to increase social fractures and take advantage of crises when they appear.[55] Daesh preferred a more decentralized approach and resorted to a redundant propaganda system in several languages, with many channels that proclaimed the advent of a regime radically breaking with Western values.[56]

Democracies were already subject to foreign interference in influencing their citizens' views and voting.[57] However, their vulnerability is emphasized by the characteristics of digital power, and they are often helpless. Identifying, influencing, isolating and opposing groups of citizens distorts the functioning of a consensus-based system. Authoritatively sharing these ideas is more effective than debating them. It is now a matter of rejection rather than development. There is no need to take military action against the opponent to impose their views. The enemy can be weakened by division alone.

The current situation could even worsen with technological advances. Reactions could be analyzed through body language, such as observing faces, to discreetly detect people's support or not of some ideas. Bots will be capable of automatically spreading false news specifically tailored to their targets. In short, international competition is expanding into the domestic political sphere in a revamped way that tends to blur the conventional

[54] G. da Empoli, *Les ingénieurs du chaos*, Paris: JC Lattès, 2019.

[55] L. Robinson, T. C. Helmus, R. S. Cohen, *et al.*, *Modern Political Warfare*, *op. cit.*, pp. 41-124. B. Jensen, B. Valeriano and R. Maness, "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist", *tandfonline.com*, 2019.

[56] L. Robinson, T. C. Helmus, R. S. Cohen, *et al.*, *Modern Political Warfare*, *op. cit.*, p. 207.

[57] E. Wilson, "Don't Call it a Comeback: Foreign Interference in US Elections has been here for years", *War on the Rocks*, 30 July 2019.

categories of war and security. Digital power could be a factor of instability on the international stage.

A revolutionary power?

Digital power is a tremendous asset for anyone who knows how to use it. It can be used for conventional activities such as subversion, espionage or sabotage, to use Thomas Rid's classification. It can contribute to military operations tactically, operationally and strategically.

However, the capability of digital power to control its target, while satisfying it, by penetrating their operational processes (the brain for people and SCADA for complex systems) is probably its greatest strength. It is most effective in the area of economic services and in political warfare for defense matters. So, its deployment corresponds less to an attempt at coercion or seduction than at subjection.

Connectivity between people or connected objects and their master is guaranteed by the network. The target itself provides the conditions for its control, by asymmetrically revealing its characteristics. This information is transformed into knowledge and power provided it can be processed and enriched. The algorithmic or psychological structure of the target becomes transparent. Identifying a vulnerability in a computer system, or a behavioral or character trait in a person can cause damage. It is enough to explore it and to emphasize it so that it becomes the weak link that diminishes the organization's general balance.

Digital power could change the forms of competition between actors in the international system in the future, as it did for economic competition. Playing on violence and physical fear to undermine the will of your opponent could appear dated in some circumstances. It is less about controlling bodies than minds. Digital power is also the power to bypass violence.

The components of digital power

Can we evaluate digital power?

Measuring digital power amounts to facing the same obstacles as in the approaches to quantifying conventional power. First, you need to have a large volume of information. Researchers at the *Global Cyber Security Capacity Centre* at Oxford University have already started collecting this type of documentation. The studies and data have been released for free access. However, they may still remain incomplete. One of the criteria of the success of cyberattacks is their stealth, so that it is impossible to rely on an accurate assessment of reality in this field.

Evaluating digital power therefore requires analysis, by examining the concept according to its different fields of application, such as defense, the economy or culture, for example. In turn, these fields of application have several aspects that have to be considered.[58] The exercise of military power on air, sea or land does not require the same skills. The same applies for digital power depending on whether it is used to spy, sabotage or even participate in war operations. However, the number of skills required can quickly become imposing depending on the comprehensiveness intended, and such a list can lose its value.

This is why authors such as J. Nye[59] or D. J. Betz and T. Stevens[60] preferred to select some capabilities they deemed essential. Nye insists, for example, on the importance of being able to conduct denial-of-service attacks and of preparing *firewalls*. Betz and Stevens observe the importance of producing standards or influencing international organizations. However, yet again, analysis is essential in identifying the deciding factors of these capabilities. R. J. Bebber, of *US Cyber Command*, considers that 25 areas contribute to the effectiveness of cyberpower.[61] The technology industry, information networks, foreign partnerships, education system, the number

[58] M. Willett, "Assessing CyberPower", *op. cit.*, p. 87.

[59] J. S. Nye, *Cyber Power*, Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010, p. 5.

[60] D. J. Betz and T. Stevens, *Cyberspace and the State: Towards a Strategy for Cyberpower*, New York: Routledge, 2012, pp. 45-53.

[61] R. J. Bebber, "Cyber Power and Cyber Effectiveness: An Analytic Framework", *Comparative Strategy*, Vol.36, No. 5, 2017, pp. 426-436.

of people involved in cybersecurity and in the digital economy are some of them. Being able to assess them requires detailed work that goes beyond the scope of this study.

Another approach consists of taking inspiration from what there is and transposing it to the digital world. Willett notes that there is much common ground between air power[62] and cyberpower.[63] Possessing the means required to protect sovereign space and avoid any aggressive action must be a component of air power and digital power. The capability to gather intelligence to assess the operational situation is another. The ability to act around the world by means of a network of air bases or the globalized connection of actors completes this brief overview. There are no academic studies that rank the different air forces, but criteria could be drawn up, such as the number of fifth-generation fighter airplanes available online or the capability to conduct long-distance punitive raids. Transposing this to the digital world, these items could be compared to the use of computers with the most powerful computing power or to the skill in penetrating protected networks. More detailed studies would be required to judge the value of such an exercise.

Deciding factors in digital power

Another approach is simply to provide the required capabilities to act effectively in cyberspace. Four elements can be put forward.

Creating a favorable ecosystem

The first element is the capability to create a favorable digital ecosystem. No international actor inherently has the qualities required to ensure its development alone. It must exploit, as we have seen, the network's collective intelligence to achieve its purpose. Therefore, it must be able to gather all these pieces of power that are distributed between all network members to concentrate them in its hands. An actor will have to exploit the hybridity of the ecosystem; that is to say, the diversity of its members who will each provide a share of the valuable, innovative – even though sometimes hostile – intelligence. It will also have to know how to manage the tension generated by this extreme spread of power and the hyperconcentration of power that it is trying to maintain.

[62] To develop this concept further, see J. A. Olsen (ed.), *Routledge Handbook of Air Power*, New York: Routledge, 2018.

[63] M. Willett, "Assessing CyberPower", *op. cit.*, p. 88-89.

Digital platforms manage to curb this tension by apparently offering advantageous services to their clients. But the state also has a part to play. It is perhaps the actor that has the most resources in this context. Admittedly, it does not have the advantages of some economic actors. For example, Google regularly recruits the best computer engineers, and has most of the data circulating on the Internet, and these algorithms work due to very high computing power.[64] It cannot be a substitute for companies, but will delegate a share of autonomy to them, to benefit in return.

Hence, the state can act as an agent. It can support doubtful projects that will be picked up and improved by private entrepreneurs, and will contribute to the national wealth. It can also invest in human capital and develop career paths that will train future actors in digital power. The field of defense can act as an incubator. The ARPANET network, an ancestor of the Internet, originally had a military purpose. It had to enable the authorities to continue to be able to interact during a Soviet nuclear attack. It benefits from contributions from fundamental research conducted by the engineers employed by the Department of Defense. Every year, *Tsahal's* Unit 8200 recruits hundreds of young Israeli cyberoperatives who respond to sophisticated attacks and retaliate in turn. They are at the forefront of research. These young Israelis, once demobilized, easily blend into the local economic fabric. They keep the Israeli digital industry vibrant due to their training provided by the state. The initial investment by the Israeli state improves its defense and increases its wealth.

The state can also play an investor and protective role, by promoting research and risk-taking in a suitable financial, legal and cultural environment. Finally, it may be a coordinator in the human, technical or organizational fields, by providing its expertise or vision when these are lacking in the private sector.

Generally, the links between the public and private spheres must be strengthened. Entrepreneurs and academics must be able to interact to promote applied research. The identification of operators of vital importance (OVIs) reinforces the overall security of computer systems in France, by imposing the necessary protective measures through regulations.

In the long term, a division of labor must clearly be established between public and private actors when they cooperate together on ambitious state projects. The state must remain the originator and outline the "what". However, the private sector will develop the "how".

[64] Interview, 10 May 2019.

In order to assume these roles, the state must be aware of the importance of digital issues and provide itself with the means to respond to them through proactive action.[65] It must know how to define its interests and to mobilize resources by outlining its priorities. This condition is essential to success.

Controlling the data

The second deciding factor in digital power is data control. It is the basis of digital wealth. But the issue is also political. Citizens provide their governments with a great deal of private information. If they are hacked, the consequences can be dramatic in the long term. For example, private healthcare companies with free access to French medical data could provide special short-term offers and threaten the sustainability of our health system. The state alone must protect this type of data.[66]

The location of data or administrative centers for this data are key issues. Discussions about establishing national *data centers*, doubts that persist about the possible dispersal of data abroad[67] or issues related to the development of sovereign *clouds* show the sensitivity of these issues.[68] They also suggest that the roles are already well allocated and that challenging the current hierarchy would require massive investment.

Maintaining the competitive edge in cyberspace

Power is also expressed by the capability to maintain the "competitive edge" in the three layers of cyberspace. The competitive edge may be physical. For example, the Chinese are monopolizing rare earths that are essential for manufacturing computers. However, they may also rely on design or technical innovation. The entrepreneurs that took the GAFAMs[69] to the top had a forward-looking vision compared to their competitors. They crushed them by imposing their solutions. From a technological point of view, the world's largest digital companies maintain close relationships with Israeli start-ups. The latter are continually improving their algorithms and maintaining their advantages over their competitors. The large companies

[65] This subject comes up regularly in interviews.

[66] Interview, 20 June 2019. See also, "La stratégie nationale du renseignement", *sgdsn.gouv.fr*, 15 July 2019.

[67] A. Cattaruzza, "Quelle souveraineté pour l'espace numérique?" *in* S. Taillat, A. Cattaruzza and D. Danet, *La cyberdéfense : politique de l'espace numérique, op. cit.*, pp. 84-86.

[68] T. Gomart, J. Nocetti and C. Tonon, "L'Europe: sujet ou objet de la géopolitique des données?" [Europe: Subject or Object in the Geopolitics of Data?], *Études de l'Ifri*, Ifri, July 2018.

[69] Google, Apple, Facebook, Amazon, Microsoft.

systematically integrate their applications into their cutting-edge products.[70]

Sometimes, the competitive edge may be maintained by the coding. Complete control of the network does not matter. It is its strategic segments that matter the most. They are the ones that must be defended with encryption. The global architecture of the systems, possibly implemented by foreign operators, must be carefully analyzed to identify the most useful or sensitive parts. Encrypting their access allows freedom of action to be maintained. A physical border is reinstituted in the network that provides a share of sovereignty.

Control of artificial intelligence (AI) is also tending to become increasingly crucial. It gives meaning, which often eludes the operator, to the exponentially increasing volume of data that is circulating on digital networks. The actors that have the most competitive models will have a cognitive advantage that they can exploit by acting earlier and more securely than their rivals.[71]

The competitive edge may, finally, be the form of the network itself. An actor may redefine its boundaries, by limiting access and controlling the interfaces with another part of the network. It isolates the users and can monitor their practices. It filters the content of data coming from outside and imposes its own rules of operation.

These actions are always expensive. Private actors sometimes provide less expensive solutions to supply such services, which may encourage them to delegate a part of their sovereignty. Such an option is incompatible with the exercise of state power that does not yield. Power is based on a goal and resources. Compromising with one or the other is already a cause of decline.

Linking digital power with other forms of power

The fourth element is paramount from an operative point of view. Cyberpower is also “the capability to use cyberspace to create advantages and to influence events in all operational environments and through all instruments of power”.[72] Digital power is only one aspect of an actor’s power. It must foster other components or succeed in linking up with them. Just as naval power boosted British might, digital power must be incorporated into a state’s key strategy in order to deliver its full potential. The digital power

[70] Interview, 30 January 2019.

[71] J.-C. Noël, “Intelligence artificielle : vers une nouvelle révolution militaire ? ”, *op. cit.*

[72] D. T. Kuehl, “From Cyberspace to Cyberpower: Defining the Problem” *in* F. D. Kramer, S. H. Starr and L. K. Wentz, *Cyberpower and National Security*, Potomac Books, 2009, p. 38.

of economic actors, although considerable, is relative on the international stage, since it lacks a sector. It does not have any influence in the military field, in cyberspace or in the real world. There is no perfect model to turn digital power into global power. Its contribution mainly depends on the links and good alignment that exist between the national strategy, economics and culture.

The United States is perhaps the most advanced nation in this field, but there is still significant progress to be achieved.[73] Indeed, it has advantages in the economic, military, cultural and ideological fields. The digital power model is liberal. It favors business expansion and wealth creation. Accumulated data indirectly benefits the defense sector. However, the links remain tenuous between private companies and the military. Cooperation seems to depend mainly on the Pentagon's financial reasons.

China is the other digital superpower. Recognizing the economic importance of this new industry, Beijing considers digital technology as a key field in its strategic competition against Washington and as a means of ensuring the political control of its people.[74] Although the Chinese state is closely backed by the private sector, it does not hesitate to punish companies when they do not act according to the Communist Party line, preferring political stability to innovation.

Other nations are more modest digital powers. Israel is successful in the economic and military field, but less interested in the cultural and ideological aspects. Russia, North Korea and Iran favor nuisance actions, but struggle to exist economically. Europe mainly acts in the field of regulation, by promoting its values through a defense of ethics in cyberspace, but is struggling to have coercive capabilities to enforce them at all times. The smooth integration of different components of digital power still remains a challenge for all state actors.

[73] V. N. Weber, "Linking Cyber Strategy with Grand Strategy: The Case of the United States", *Journal of Cyber Policy*, published online on 17 August 2018.
[74] N. Inkster, "China's Cyber Power", IISS *Adelphi* 456, New York: Routledge, 2016.

How the real world influences the virtual world

The military response

The effects of digital power have sometimes been difficult to contain in the field of defense and security. However, some signs show that the situation is gradually changing.

Cybersecurity, for example, is getting tougher. Defense is increasingly organized in the background to defeat attacks, with the creation of labyrinths in computer systems to mislead the hacker. The security of these systems is also taken into account when they are designed. The addition of patches on programs often came down to renovating software's facade rather than redesigning its foundations. Its effectiveness was relative. Now, shields are incorporated into software design, complicating the infiltration and implantation phases.

Progress is also being made in the area of attack identification and attribution, although discretion surrounds this sensitive area. Admittedly, obvious proof immediately pointing to the origin of an attack is rare. Doubt remains. However, with time, experts have gained more and more useful information to distinguish the traces left. The number of hackers capable of acting at the high end is limited, although this community is always shifting. They are not increasing. Each one has a style and preferred modes of action that are equally clues to trace them. The phenomenon of extreme concentration that we have already observed for platforms or the number of influential bloggers on the Internet can be turned into a weakness.[75]

Public attribution of attacks remains a political decision. Although France is cautious, the United States decided to review its policy. Washington, in cooperation with other Anglosphere capitals, for example, rapidly attributed the *NotPetya* virus to teams of Russian military hackers in February 2018. In 2018, the Department of Justice accused eight teams of Chinese, Russian, Iranian or North Korean hackers compared to only one

[75] Let us emphasize the fact that all of these comments are mainly about the high end of cyberdefense. In the area of cybersecurity, many actors have reduced capabilities and remain vulnerable to hordes of certainly less talented hackers, but who remain successful enough to regularly improve their modes of action and to threaten the operation of businesses for criminal purposes.

in 2014.[76] The consequences of increased *naming and shaming* and legal proceedings are rather low in the short term. The accused can deny the accusations and demand solid proof of their involvement. Nevertheless, in the longer term, such a position could boost cooperation between some states, speed up discussion about establishing common rules in cyberspace and damage the image of some actors on the international stage.

This determination by the United Sates seems to extend to all areas of cyberdefense.[77] The US rules governing the activation of offensive cyberoperations are becoming laxer. In order to stem the multiple attempts to penetrate US digital networks, Washington threatens to counter-attack by neutralizing the attackers' computer systems. The risk of escalation exists, although Defense Department officials insist that relaxing the rules did not imply cyberspace becoming a Wild West.[78]

Forms of deterrence in cyberspace are gradually emerging.[79] Deterrence, which refers to the act of preventing an opponent taking action, will not know how to prohibit any action in the digital space. It can only be designed from a threshold or volume of operations. It could be organized in the manner of a police force that has to ensure the maintenance of order in a public space. The attacker must know that some acts will systematically be reproved, depending on their frequency and scope.[80] For example, Nye suggests that standard taboos be defined that different actors would be committed to comply with. He also believes in the value of deterrence by entanglement: the interests of actors in the digital sphere are so intertwined that an action in one area may end up harming the attacker in another field because of the consequences that it may trigger.[81]

Nye thinks that cyberdeterrence can be exercised entirely in cyberspace. This point is one of the key issues for consideration in future years. The Western powers have for the time being made responsible and moderate use of their digital and physical capabilities to manage abuse in cyberspace. But their reactions could increasingly extend to the real world, whether in the context of deterrence, coercion, or more simply military affairs. In 2015, J. Hussain, one of Daesh's main hackers, was killed by a drone for specifically

[76] K. Charlet, "How the US Approach to Cyber Conflict Evolved in 2018 – and What Could Come Next", *worldpolitics review.com*, 26 December 2018.

[77] *National Cyber Strategy of the United States of America*, Washington DC: The White House, September 2018.

[78] K. Charlet, "How the US Approach to Cyber Conflict Evolved in 2018 – and What Could Come Next", *worldpolitics review.com*, 26 December 2018.

[79] French strategic vocabulary retains the term "discouragement" to mark the difference with nuclear deterrence.

[80] S. Taillat, "Dissuasion et coercition", *op. cit.*, p. 144.

[81] J. Nye, "Deterrence and Dissuasion in Cyberspace", *International Security*, Vol. 41, No. 3, 2017.

publishing information about US personnel online.[82] At the beginning of May 2019, a building hosting Hamas' cyberoperators was destroyed by an Israeli air strike to prevent a cyberoffensive against Israeli targets.[83] The Western powers' thinking is more focused around the impact and effects produced by cyberattacks than the resources used to carry them out. According to them, there is no longer a disconnect between the virtual and the real.

Moscow and Beijing reject this approach and accuse the Western powers of wanting to militarize cyberspace. The Russians and Chinese would like to retain their freedom of action and benefit from the asymmetrical resources offered by this virtual environment. They have no interest in extending conflicts to the real world, where their inferiority to US forces is still evident. The cost of an attack could become prohibitive.

The advantage that the attackers have in cyberspace is therefore being challenged. Initiatives taken in this field could indicate that a new digital phase will be announced.

Searching for new regulations

A similar reaction movement seems to be developing in other digital sectors. States are testing many types of strategy to weaken the hyperconcentration of power of some private actors and rebalance the distribution of wealth created by their development.[84]

An initial position is direct confrontation. This is one of the measures that France has chosen, by imposing the GAFA (Google, Apple, Facebook, Amazon) tax, before the OECD takes this initiative. The lack of enthusiasm of other European countries and the risks of corporate relocation or retaliation by the US administration show that the success of such a measure is not guaranteed. However, other more radical expressions of this strategy must not be neglected over time. The promulgation of an anti-trust law in the United States could defeat the digital platforms and reintroduce competition where it has disappeared.[85]

A variation of this position is the creation of national or continental champions who will compete with established companies. The French search engine *Qwant*, one of whose characteristics is not to trace its users, is an example of this. The desire to promote a European champion in the

[82] Z. Doffman, "Israel Responds to Cyber Attack with Air Strike on Cyber Attackers in World First", *forbes.com*, 6 May 2019. I would like to thank B. Pajot for alerting me to this event.

[83] *Ibid.*

[84] Interview, 12 July 2019.

[85] "Domestiquer les géants du numérique", *Le Monde*, 12 September 2019.

race for 5G is another. Following this pathway, however, is difficult, given the income that the large platforms already enjoy. The entry fee is high for questionable chances of success.

"Soft regulation" is another option. The European Union (EU) is pursuing this with the introduction of the General Data Protection Regulation (GDPR). GDPR is an extraterritorial law that allows standards corresponding to the EU's values to be imposed in cyberspace. The interests of EU citizens are defended regardless of where they connect in the world. The individual retains sovereignty of their data by agreeing to share it and receiving assurance that it will be protected. The breach, even unintentional, of this principle can be costly for companies. *British Airways* was punished with a fine of around 200 million euros after it was the victim of hacking that swallowed up the financial data of about 500,000 of its clients.[86]

A final possibility is to coordinate with the platforms to set modes of operation approved by everybody. The report on the regulation mission of social networks, known as "Mission Facebook" and led by Benoit Loutrel, is an example of this.[87]

Civil society is not inactive for its part. The development of *Open Source Intelligence* (OSINT) sites is producing impressive results that stigmatize the action of private companies or states. *Bellingcat* is one of them. Its members have managed to prove Russia's involvement in the destruction of *Malaysian Airlines* flight MH 17 over Ukraine despite Moscow's repeated denials.[88] Working in all transparency, by exploiting data made available to everyone on the Internet, the OSINT sites can nowadays gather and process data more effectively than the CIA or the KGB could do a generation ago.[89]

It is still too early to say whether such practices herald a new form of political participation by citizens pushing for transparency or whether state initiatives will curb the expansion of large digital platforms. The defense of values is not always enough when it is not supported by proven political or military capabilities. Nevertheless, these attempts to establish another rationale in cyberspace show that the sense of history may be reversed and that the real world is increasingly trying to impose itself on the virtual world.

[86] D. Filippone, "Violation RGPD : une amende de 200 M d'euros pour British Airways", *Le Monde Informatique*, 8 July 2019.

[87] "Régulation des réseaux sociaux-Expérimentation Facebook", *economie.gouv.fr*, May 2019.

[88] P. W. Singer and E. T. Brooking, *Like War: The Weaponization of Social Media*, *op. cit.*, pp. 71-77.

[89] *Ibid*, p. 75.

Digital technologies and the business cycle

To better understand the transformation of the old dynamics, it is stimulating to change scale and to consider the advent of digital as a technological revolution, like the industrial revolution, or the more recent introduction of steam, steel and oil in production cycles.

For this reason, Carlota Perez's studies on the impact of technology on business cycles provide a model that can account for current developments.[90] It shows that these technological revolutions generate cycles regularly consisting of two phases separated by an inflection point. In the first phase, the new technology gradually takes the place of another older one. Its applications are many and appealing, and the returns on investment are high. The inventors' enthusiasm maintains unbridled enthusiasm. This excitement is shared by entrepreneurs trying to satisfy their hubris and financiers in search of easy and immediate profits. The latter collect most of the wealth, dominate the scene and increase bubbles of prosperity based on weak foundations.

This period of euphoria suddenly ceases when these bubbles burst, causing a recession. This is the time of the inflection point, corresponding to the period when private and collective interests clash to find a new balance. The duration of this stage is variable, and depends on the balances of power between the different actors involved in controlling the technology.

This inflection point usually heralds a second phase, called the Golden Age by Carlota Perez, when this balance of power has stabilized in the sense of the common interest. The control of investments becomes more institutional and passes over to the industrialists, supported by state authorities. The technological applications are supervised and regulated so that prosperity is shared out better. This Golden Age will end with the emergence of new technologies.

We may now be going through the inflection-point period. The American superpower's proactive approach in the field of defense is an indicator of this. The search for solutions to control the GAFAMs or civil society initiatives to impose more transparency are others. Digital power is a power that could be contained in the future.

[90] C. Perez, *Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages*, Cheltenham: Edward Elgar Publishing, 2003.

Towards a more distinct fragmentation?

However, business cycles do not put an end to international competition. This remains with the divided actors, supporting opposite approaches on geography and the governance of cyberspace. Some, such as China and Russia, consider cyberspace in Hobbesian terms. It does not have any influence in the military field, in cyberspace or in the real world. They support state governance, which they believe alone can uphold the notions of sovereignty and security, the foundations of a harmonious international order. The organization of the International Telecommunication Union is their model. The problem is that this frantic quest for order can hide much more perverse forms of authoritarianism that undermine the current operation of the digital world.

Others, like the Anglosphere countries, prefer a more decentralized approach. They want all the actors in the digital world to be able to contribute to its operation. If everyone is involved in setting the standards, rules and sanctions around a negotiating table, they will be more inclined to comply with them. The legitimacy and authority of regulatory institutions will only be better. However, the Snowden Affair, which showed the collusion of interest between the United States and some private actors, has weakened this vision.

Also, the risk of partitioning cyberspace is real. It is even fragmenting, if you consider that the Russian and Chinese Internet are partly disconnected from the global network. Digital power could fragment. The governance of digital space could vary depending on the area and be determined in the future between regional organizations of states with similar political systems. One of the means to safeguard some common international rules may be to seek to produce standards for limited and restricted fields, such as intellectual property for example, without major immediate strategic issues.[91] However, the trend seems to be the creation of two distinct digital spaces.[92] The standard geopolitical opposition between a *Heartland* and a *Rimland*, between a finite part, closed in on itself, and another one more open, which surrounds it, could find a new lease of life.[93] However, its outcome remains uncertain.

[91] S. Patrick, “The Unruled World: The Case for Good Enough Global Presence”, *Foreign Affairs*, Vol. 93, 2014, pp. 58-73.

[92] Interview, 5 July 2019.

[93] N. Spykman, *Geography of the Peace*, San Diego: Harcourt, Brace and Company, 1944.

Conclusion

Digital power is a complex and multi-faceted subject. It is a power both conventional and network-based, liberating and controlling, shared and fragmented, asymmetrical and contained, fragile and transient, but which can bypass obstacles. It is continuing to evolve as people invent new practices.

Its future will mainly depend on the development of new technological applications. Artificial intelligence will play a decisive role. The automation of some tasks could be increased, requiring a rethinking of the relationship between people and machines and between digital space and the real world.[94] Computers' calculating power could change scale with quantum computing. Software encryption, which is one of the current preferred solutions for protecting computer systems, could easily be undone. 3D printing could revolutionize the way items are produced and increase individuals' power. The nanosciences will accelerate the miniaturization of the world, perhaps starting a new cycle, in Carlota Perez's sense.

The forms of digital power will also depend on political choices. In the short term, the still unclear concept of digital identity will probably spark debate. People are already identified by their fingerprints or biological characteristics. Can people's data that they share on networks eventually be based on a digital identity? Regulating the use of this data will be essential. An operator with access to this data will be able to digitalize a person's past and anticipate their future by extrapolating the knowledge.[95] Those in possession of the data will even be able to distort or erase it, therefore condemning themselves to virtual death. The right to be forgotten or to be remembered on the Internet could become two fundamental rights. But how to enact them? In the longer term, other debates, like the programmed advent of the enhanced human, will surely become inevitable.

[94] J.-C. Noël, "Intelligence artificielle : vers une nouvelle révolution militaire ? ", *op. cit.*

[95] P. Bellanger, *La souveraineté numérique, op. cit.*, p. 101.

1979
2019

ifri

French Institute
of International
Relations