Digital Sovereignty

Europe Challenge for a Strategic Technical Autonomy

Paulo Moniz

| Digital Global Unit Security & IT Risk da EDP;
| Membro da Direção da CIIWA;
| Vogal da Direção da EuroDefense-Portugal.

Abstract

The concept of Digital Sovereignty has recently emerged as result of the increasing importance and dependence of our societies in technology, and the concerns for States to promote strategy autonomy in the digital realm. This article intents to demonstrate how Digital Sovereignty is fundamental in today's world, and in Europe in particular, to ensure our safety, comfort, and prosperity, preserving shared values that we have conquered throughout our history. To achieve this objective, it starts by introducing a framework for cyber power and the scenarios where it is, and can be, applied, followed by an analysis of confluence points in cyberspace, where cyber power can be leverage, throughout the cognitive, information and physical layers of this domain. This work finalizes pointing out to an overview of what Europe is doing and can do to maintain its strategy autonomy with focus on resilience.

Context

Sovereignty, in political theory, is the ultimate overseer, or authority, in the decision-making process of the State and in the maintenance of order (Encyclopedia Britannica, 2022). We might also find other definitions related with population, a territory, a government, and independence.

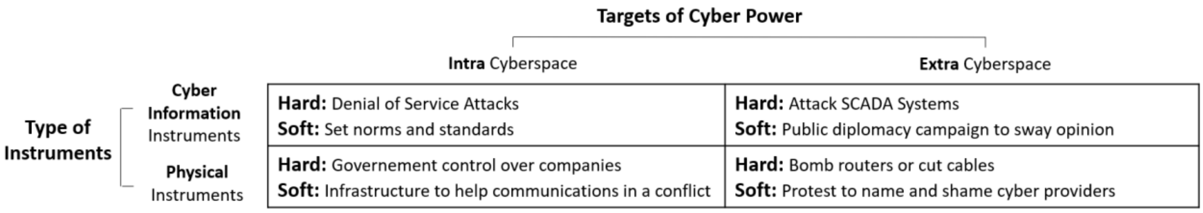
In the new world, increasing dependent on technology, the concept of territory crosses the conventional boundaries we usually know, into the cyberspace, where most the society activities and essential services are moving to. Maintaining authority, order or independent decision making in such realm, demands that governments control how technology is used to support our lives as citizens in a democratic society.

There is a growing and fact-based concern that we, Europeans, are gradually losing control over our data, our capacity for innovate or our capability to protect critical infrastructures and essential services operation (MADIEGA, 2020). Giant technologies companies are mostly from USA and China, and they are managing cloud services for all world, but also manufacturing servers and communications' equipment that we use in our companies, in our homes or in our institutional services. Even knowing that a relevant number of this vendors and service providers are based in friendly countries, with whom we share values, not having the ability to act independently in the digital world might pose short and long-term risk to our European's society.

This way, the **Europe's ability to act independently in the digital world**, shaping and enforce legislation in its environment, is an upmost and urgent discuss, demanding a deep understand of the challenge, a continuous monitoring of situation as also short and long-term actions to overcome the risks.

Cyber power framework played-out in today's world

To understand the ways Digital Sovereignty could be threatened it is fundamental to be aware of cyber power and how it can be used. Cyber power can be defined as "the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power" (Nye, 2010). To provide a structured analysis of cyber power, is proposed the following framework, where one dimension stands for the target domains and other for the type of instruments of power.



		Targets of Cyber Power	
		Intra Cyberspace	**Extra** Cyberspace
Type of Instruments	**Cyber Information** Instruments	**Hard:** Denial of Service Attacks **Soft:** Set norms and standards	**Hard:** Attack SCADA Systems **Soft:** Public diplomacy campaign to sway opinion
	Physical Instruments	**Hard:** Governement control over companies **Soft:** Infrastructure to help communications in a conflict	**Hard:** Bomb routers or cut cables **Soft:** Protest to name and shame cyber providers

Figure 1 - Cyber Power Framework (adaptation from Nye)

Cyber power can **leverage cyber or informational instruments** within the cyberspace to produce **outcomes within it** or in **other domains outside cyberspace**. It is also possible to **use physical**

instruments of power, i.e., non-cyberspace instruments, to produce **effects within** and **outside the cyberspace**.

We can use, as analogy, the sea power, where naval resources in the oceans can be used to win naval battles, as also to influence, out of seas, commercial activities, or public opinion, only by the way you position your ships' squadron in international waters.

It is also possible to **use physical instruments of power**, non-cyberspace instruments, to **produce outcomes within** and **outside the cyberspace**. Using the same sea power analogy, we can conceive a political decision by a countries' President ordering ship's fleet withdrawing or the use of land weapons to hit air communications equipment that support naval resource's operations.

Illustrating with examples, the DoS attacks (Denial of Service Attacks) that Russians are executing against Ukraine supporting States (Doyle, 2022), is an example of **the usage of instruments of power, within cyberspace**, to produce **outcomes in the cyberspace itself**, while the malware used in 2015 against an Ukraine energy utility, disrupting their operations and letting part of Ukraine without energy, also performed by the Russians (Zetter, 2016), shows the **use cyber instruments** with **impacts outside the cyberspace**. Considering this last type of cyber power usage, is also interesting to mention the Russian interference in American elections, where social networks on the internet were manipulated to influence public opinion against the democratic candidate (Hosenball, 2020).

As an example of the **usage of non-cyberspace instruments of power**, we can recall a recent major cable cut in the south of France that has disturbed internet connectivity to Asia, Europe and US (King, 2022). The **impact was in the physical domain**, yet with latter repercussions on the cyberspace. Still **using non-cyberspace instruments of power**, but this time with **impacts in cyberspace**, we have the Elon Musk decision to open the satellite communications to support Ukraine military operations, with obvious impacts it the course of the war (Fox & Probasco, 2022). A political decision, made by a private company, that directly provides a communications infrastructure for one of the conflict opponents!

One could argue that the involvement of private companies in war conflicts is not new and recall, as an example, that in World War 2 the Ford Motor Company helped build the equipment needed by the military, such as vehicles, aircraft engines (Fox & Probasco, 2022). However, this service was requested by governments, today, individuals like Elon Musk, decide, by their own perception and judgment of the conflict, to help States or other groups, potentially changing the course of a battle. Nowadays it is unquestionable that military and security operations are more tied to technology than ever before, but also that this technology is backed by private company businesses, allowing them to have independent power and the will to act politically, which is something that also never happened in the past with this intensity.

Thus, we may conclude that cyber space is not just an area for opportunities, competion and collaboration, but becomes a battlefield for control of, industries, markets, values, influence and, ultimately, our way of life.

Cyberspace, a domain with confluence points

After understanding, with real examples, what cyber power is and how it has been exercised in today's world, we must now dive-in cyberspace particular characteristics, understand which makes it a complex and unique domain that could change the current world order, given enormous advantages for those nations or organizations who control its environment.

A common question that raises discussion, concerns whether cyberspace is a Global Common. Global Commons are domains that are not controlled by any State yet are shared and universally needed to support society's regular and increasing flows of information, commerce and people (Buck, 1998). Traditionally, global commons included the high seas, airspace, and outer space, but recently in our history, some argue that cyberspace has that status as well.

Cyberspace has a distinguish characteristic that is the first domain created by the humankind and, despite the universal access provided at higher internet abstraction layers (WWW - World Wide Web protocol), it also relies in physical infrastructure (hardware servers and cables) located within the boundaries of sovereign States. Considering this fact some claim that cyberspace could not be a perfect Global Common since a public good is one from which all can benefit and none excluded, which is not the case of cyberspace (Nye, 2010).

More important than classifying cyberspace as a Global Common or not, is to assume that, in fact, it provides a common global set of resources, fundamental to ensure the progress and well-being of today's societies. It is a domain that it is crucial to defend, to allow a safe and reliable use, but to achieve this goal it is necessary to understand its confluence points that represent vulnerabilities in the functioning of current societies.

Confluence points in cyberspace

In all domains it is possible to identify confluence or convergence points, which represent concentrated areas where people and goods flow along converging lines. For example, we can identify seaports or straights that connect two vast seas. Controlling these points is an exercise of power. In cyberspace we can also find the same concept and, as will be seen, with clear threats to the sovereignty of nations.

A structured analysis requires the division of cyberspace into three layers, as in the cognitive pyramid below (Nunes, 2020), where the bottom layer concerns infrastructure and data, the **physical domain** of cyberspace, while the layer immediately above has to do with **information** and its **domain**. The top layer concerns the use of information to create knowledge and wisdom, in what is dubbed the **cognitive domain**.

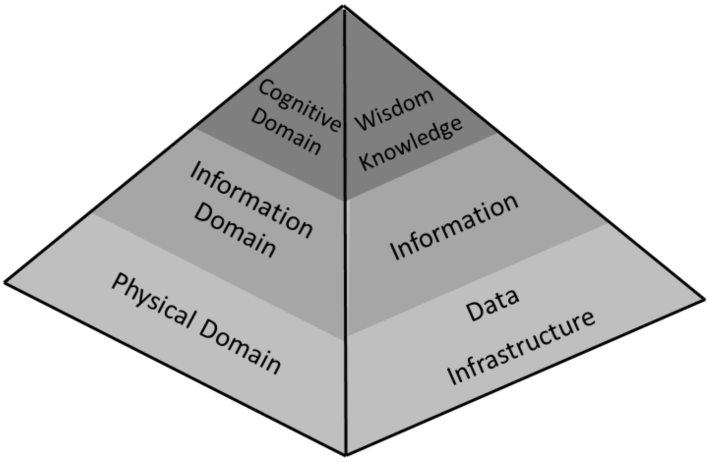


Figure 2 - Cognitive pyramid (adaptation from (Nunes,2020))

Physical Domain

The physical domain layer comprehends all the hardware infrastructure, composed by computational resources and all data signals connectivity between them. The connections between devices creates networks, which interconnects with other networks, building networks of networks and, ultimately, the internet. At this layer the effects are at physical level, on hardware, like cables that transport signals, satellites systems, routers that interconnects networks or endpoints processors, such laptops, servers or even cloud service providers providing infrastructure services (IaaS - Infrastructure as a Service).

Considering the current global reality, one can identify, for networks, huge vendors that provide equipment, like Cisco and Huawei and, for laptops, Lenovo, HP and Dell. All these companies are non-European, making more difficult for Europeans to impose standards and requirements on those devices.

When it comes to infrastructure cloud service providers, AWS, Azure, Google and Alibaba, based in the US and China, account for more than 70% of the global market (Richter, 2022), leading Europeans, as well as other countries in the world, to rely exclusively on these technology giants.

As for satellite networks, which play a key role in today's global communications, and can be used in conflict to give advantage to some parties, as described earlier in this article for the situation in the Ukraine conflict, the playing field is more level, as we can rely on European companies that manufacture and operate satellite networks. However, for 5G, the situation is not as good, since the core of network communications is mainly based on American and Chinese suppliers, just like the 4G networks that are used daily in our lives (European Commission, 2019).

Still on this physical domain there is a strong concern about Europe's ability to fulfil its own digital technology needs in terms of hardware acquisition in the civil and militarily realms. Dependences in the supply chain are critical and the risk of supply chain disruption are real and threatens our autonomy (European Commission, 2019). These disruptions can be caused either, unintentionally, such an external and uncontrollable event, like the Covid pandemic, or natural disasters, but also intentionally, resulting, for instance, from political hostile supply embargos in a war context. In the current situation there is a strong dependence on microchips manufacturing which are essential for all the devices thar supports internet as also our computational resources at our companies and personal lives.

In addition to the threat of supply chain disruption, there is also a risk that compromised equipment could penetrate critical digital infrastructures in the EU, with serious cyber security implications (European Commission, 2019). Considering that threats, as well as critical services, are interconnected and transnational in nature, vulnerabilities in one Member State can have cross-border repercussions or even affect the Union as a whole, which means that an equivalent level of protection needs to be provided by all Member States.

In all these examples described in this physical domain we found confluence points that are controlled by non-European companies or countries, which makes us at merci of those entities to exercise cyber power at their will.

Information Domain

With respect to the information domain, it covers all the systems that support and manage the entire operation of computers and networks, but also all enterprise or personal use software. It includes all operating systems for laptops and cell phones, communication protocols such as DNS (Domain Name Service), which are critical to the operation of the Internet, or cloud services from a Platform as a Service (PaaS - Platform as a Service) perspective. Enterprise systems relevant to the scope of this paper, comprise applications that manage data to produce information for a higher layer of knowledge and wisdom, such as business intelligence platforms or decision information systems.

If for the enterprise systems we can't identify a clear predominance from few vendors or countries (even Europe counts with global giants such SAP or Amadeus), considering the operating systems, similar in what happens with infrastructure, all the big players that dominate the entire market are non-Europeans, either for mobile phones or laptops, where Google, Apple and Microsoft cover almost of all the existent devices (Taylor, 2022). In the platform cloud service providers' realm (PaaS – Platform as a Service), the same names repeat: AWS Microsoft and Google.

To understand the threat posed by vulnerabilities in operating systems and the technology monoculture approach, we can recall the WannaCry ransomware attack. A worldwide cyber-attack in May 2017 by WannaCry ransomware, targeting computers running the Microsoft Windows operating system. The WannaCry ransomware impacted more than 300,000 machines in 150 countries, all running the same vulnerable versions of operating systems, including 80 NHS hospitals in Britain, which were forced to divert patients after the malware prevented clinicians from accessing medical records (Palmer, 2021).

Confluence points at this level can lead to extremely costly impacts on society. We are dealing with logical effects on systems, but those systems may be controlling critical infrastructure such as energy management, transportation, or water supply, to name a few. Exploiting common logical vulnerabilities, which represent points of confluence, can cause physical impacts, a case where we are exerting power using information resources in cyberspace to produce results in the physical realm.

Cognitive Domain

At this level, information takes context, creating the knowledge used to induce perceptions as well as driving decisions. Systems and applications at this level are Internet search engines, social networks, AI (Artificial Intelligence) algorithms, or autonomous devices. At a higher level in this layer, wisdom is used to create laws, regulations, or frameworks.

Analyzing search engines, the use of Google is completely overwhelming across all the western world and Baidu dominates in China's territory (Chris, 2022). Regarding social networks, the ones most used are Facebook, YouTube, Whatsapp or Instagram (Chaffey, 2022). All these social networks are owned by American companies and in China is mostly used Sina Weibo and TikTok. Again, we find confluence points in few applications from non-European countries, practically a bipolarity. It's also relevant to acknowledge that the use of social networks could be extremely dangerous in what concerning the protection of our democracy, as it was well demonstrate in the Russia interference in America elections.

However, there are fields where Europe has played a leading role in the definition of laws and regulation, being the GDPR (Data Protection Regulation) or the NIS (Security for Networks and Systems) very good examples.

How to control Digital Sovereignty's risks

To change the scenario described we first need to recognize that the current world context, that seems to lead to a loose of European autonomy, is not inevitable. We need to understand risks and threats and establish actions to consistent pave another path for our society.

Main EU action taken

Governments are already concerned about this challenge and several actions are already underway. Considering innovation and the data economy, "Horizon 2020" was an EU research and innovation program with almost €80 billion of public funding, spread over seven years (2014 to 2020) funded initiatives on key technologies such as 5G, big data or cloud computing, among others. This program has a successor, "Horizon Europe," which will run until 2027, with a total budget of €95.5 billion (MADIEGA, 2020). In addition, the data strategy adopted in February 2020 will ensure that more data becomes available for use in the economy and society, while maintaining control of data in businesses and individuals.

In the military realm the Permanent Structured Cooperation (PESCO), established in December 2017, is the part of the European Union's (EU) security and defence policy. It joins 25 Member States, currently with 60 projects running, aiming to increase collaboration between Member States and to develop defense capabilities to undertake the most demanding missions, thereby provide an improved security to EU citizens.

When it comes to data privacy, the EU has adopted a very demanding framework for privacy and data protection, with the General Data Protection Regulation (GDPR), imposing stringent requirements regarding individuals' personal data, leading to multinationals to adopt protection controls in their services as well.

For cybersecurity, the 2016 Network and Information Security Directive (NIS), now with an evolution being deployed (NIS2), improves Member States' cybersecurity capabilities and cooperation and imposes measures on companies to prevent and report security incidents and cyber-attacks in key sectors (i.e. energy, transport, banking, financial market infrastructures, the health sector, drinking water supply and distribution and digital infrastructure).

Aiming to provide more trust in the supply chain, the European Cybersecurity Act, passed in 2018, creates an EU-wide cybersecurity certification scheme for ICT products to protect consumers and businesses from cybersecurity threats. This is an example of the EU leading the way in cybersecurity reference frameworks definition, forcing third countries, as well as private companies doing business in the EU, to update their cybersecurity practices and policies to ensure compliance. In the same vein, another relevant initiative is the adoption of a recommendation in March 2019 for a common EU approach to 5G network security and the subsequent publication of a toolbox on 5G cybersecurity in January 2020 (European Commission, 2020).

In resume there are already several proposals rolling-out for industrial policy, domestic technology development projects, rules to limit foreign companies, data localization, critical infrastructures protection requirements and essential services operators' cybersecurity policies or even more aggressive jurisdictional regulations such the afore mentioned GDPR. All these initiatives are extremely important however them will take time to produce effects and might not be enough or, if not applied in a reasonable way, have adverse effects.

Some actions we are putting in place to defend Digital Sovereignty, such increased internal control over technology has the potential to create serious costs (Ilves & Osula, 2020). Technology autarky and even simple localization rules break global supply chains. New legal requirements create compliance costs for domestic companies as well, and industrial policy can lead to costly technology choices, don't forgetting that other countries' policies can also hurt our own companies. So, we must be carefully when applying these policy mechanisms in order not to create disadvantages for European companies and citizens.

Thus, we need to create urgency to protect ourselves from the confluence point in the cyberspace, reinforcing and developing a key approach for digital strategic autonomy: **Resilience.**

Resilience is key for autonomy

It's clear that the Digital Sovereignty is a challenge that needs to be addressed at a global level by governments and international organizations, from civil to military realms. Notwithstanding the need of a global approach by the relevant authorities, at organizational level we can, and should, start to act to defend our Digital Sovereignty, especially if our organizations manage critical infrastructures or operates essential services to society. Wait to act could be too dangerous!

In every meeting, in every decision in our organizations or even in our private lives, we should always consider the principles of resilience, throughout the construction of systems up to application operations, but also in the design of business services, including people skills. Resilience includes, among other considerations, good **situational awareness**, **analytical monitoring**, **segmentation**, **diversity** (NIST, 2021) and **coordinated cooperation**, which should be considered across organizations, sectors and Member States.

At EU scale, good **situational awareness** implies a better understanding of Europe's vulnerabilities and dependences, mapping critical infrastructures and essential services across all countries. To achieve this objective is required a framework of cooperation between public and private sector, where trustable, timely and actionable information should flow between agents. We are still far away from this objective. There exist groups, fragmented, that joins some entities from specific sectors, but we are lacking a structured and efficient collaboration.

It's also crucial to maintain a list of critical information technologies that are of high importance to the EU's strategic autonomy and identify risks related with their supply. For those technologies we might need to foster industry investments to address specific solution, or simply considering alternatives partnerships for supply, or even substitution by other solutions.

At organization level the same principles should apply, addressing **situational awareness** by identifying business dependencies on services providers, technologies and materials. It's also crucial for organization to promote the participation in trusted information sharing communities in order to better contextualize threat environments for the organization.

The **analytic monitoring** is also fundamental for the defense of our infrastructures. Monitor and analyze a wide range of behaviors and properties, in a continuous and coordinated way. Like the situational awareness, analytic monitoring can be applied at EU dimension, for instance to detect hybrid threats (Savolainen, 2019), but also at organization level, with a careful and deeper monitoring of essential assets that supports critical business functions.

Segmentation is another approach that organizations should take in consideration while designing and developing their services and all technology that supports them. It's crucial to define and separate systems elements based on critically and trustworthiness. This principle can also apply across diverse domains but, at least in organizations, is fundamental to contain adversary activities, limiting, for example, possible targets to which a malware on a compromised system can propagate.

Diversification, the use of heterogeneity to minimize common mode failures, as the example above of wannacry ransomware. With this approach we should aim to limit the possibility of the loss of critical functions due to the failure of common components among our critical networks. This principle might algo apply to another organization levels and help to prevent supply chain disruptions.

European citizens are key when it comes to build resilience. It's obvious that individuals participate in all the three cyberspace layers here presented, however, in the cognitive level, it's extremely important that they are prepared for the use of new technologies. Nowadays, leverage by the technology apparatus, we are constantly overloaded with news and information from different origins and formats, some, as also here mentioned, manipulated to create opinions and shape behaviors in a harmful way, so it is critical, for defense of our values, that we are prepared to analyze and make critical thinking in every single bit of information that is presented to us, regarding different aspects such content, opportunity or source. It also fundamental to understand our rights and duties as citizens, and how they are being played out in the cyberspace, in order to foster our attitude to demand our data protection, as in the case of aforementioned GDPR, but also to pressure organizations and governments to consider cybersecurity and digital ethics in the products, solutions and services they develop, especially in the AI (artificial intelligence) and autonomous devices fields. To achieve this, it's necessary to establish training and awareness programs in digital areas for citizens across all Member States, starting from basic schools. They should level all European citizens capabilities and competences in the technological field because, as in the infrastructures and services, we are tightly interconnected, and events, like public opinion, in one country, can easily propagate to others. That can only be successful implemented if we have **collaboration**.

Coordinated collaboration underlines every single approach towards strategic autonomy and resilience build. Cybersecurity and cyber resilience require a collaborative attitude across all levels, from civil to military realms, as also from individuals to Member States, including organizations, public and private companies, that plays a key role in our technological society. Resilience doesn't solve lack of investments in new technologies or the lag we already have in the cyberspace presence, namely in some domains like operating systems or internet search engines, however, it allows us to be better prepared for any cyber power exercise in confluence points, while some bold initiatives take place.

There is no doubt that companies are made to be profitable and to achieve this objective it is necessary to optimize resources, but it's also crucial for us to understand what critical services we are delivering to society and what are our responsibilities, considering both safety and security to protect our values. Technology, today, underpins our way of live, supports progress, economic growth and well-being. Govern the technology environment is fundamental for our sovereignty, our digital sovereignty.

Conclusion

Threats are changing rapidly in the world where technology underpins the ways we communicate, how we trade and how we live. Cyber space is not just an area for opportunities, competion and collaboration, it becomes a battlefield for control of, industries, markets, values, and influence but, ultimately, our way of life.

Some Nations or organization might use cyberspace, controlling its confluence points, as a domain for leverage intelligence, military operation or to influence and shape the world economic ecosystem as also public opinion at their will. Dominate the technology field gives a huge geopolitical advantage for those that realize it first, as our common history demonstrates. As Europeans we cannot falling behind, we need to endeavor a collective action to achieve our strategic autonomy concerning the digital.

The bad news is that, in fact, we seem to be lagging, considering all the control of confluence points already established in the cyberspace, however, for the good side, is that we, Europeans, despite that we have several crucial overarching initiatives in place, we can start to act right now, every day, as individuals and organizations, building resilience.

We need to standup together to protect the most critical infrastructure of our societies: Our democratic values!

References

Britannica, T. Editors of Encyclopaedia (2022, August 26). *sovereignty*. Encyclopedia Britannica. https://www.britannica.com/topic/sovereignty

Buck, Susan J. (1998). *The Global Commons An Introduction*. Island Press, Washington DC.

Chaffey, Dave. (August 22, 2022). *Global social media statistics research summary 2022*. https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/

Chris, Alex. (October 24, 2022). *Top 10 Search Engines In The World (2022 Update)*. https://www.reliablesoft.net/top-10-search-engines-in-the-world/

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Doyle, Peyton (2022). *Major DDoS attacks increasing after invasion of Ukraine*. https://www.techtarget.com/searchsecurity/news/252521150/Major-DDoS-attacks-increasing-after-invasion-of-Ukraine

EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

EU Regulation 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

European Commission, European Political Strategy Centre, (2019). *Rethinking strategic autonomy in the digital age*. Publications Office. https://data.europa.eu/doi/10.2872/231231

European Commission. (2020). *Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures*. CG Publication. Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468

European Union Institute for Security Studies, Missiroli, A., Fiott, D., Tardy, T. (2017). Permanent structured cooperation: what's in a name?, Publications Office.https://data.europa.eu/doi/10.2815/996506

Fox, Christine H. and Probasco, Emelia S. (October 19, 2022). *Big Tech Goes to War: To Help Ukraine*, Washington and Silicon Valley Must Work Together. Foreign Affairs.

Hosenball, Mark (August 19, 2020). Mohammed, Arshad (ed.). *Factbox: Key findings from Senate inquiry into Russian interference in 2016 U.S. election*. Reuters. Washington. https://www.reuters.com/article/us-usa-trump-russia-senate-findings-fact-idUSKCN25E2OY

King, Chris (October 23, 2022). *Serious incident involving CUT underwater cables in South of France affects internet worldwide.* https://euroweeklynews.com/2022/10/23/serious-incident-involving-cut-underwater-cables-in-south-of-france-affects-internet-worldwide/

L. Ilves and A.-M. Osula. (2020). *The Technological Sovereignty Dilemma – and How New Technology Can Offer a Way Out*, European Cybersecurity Journal.

MADIEGA, Tambiama André. (2020). *Digital Sovereignty for Europe*. European Parliament.

National Institute of Standards and Technology (NIST). (December 2021). Special Publication 800-160 Vol. 2 Rev 1. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final

Nunes, P.F.V. (2020). A Edificação da Capacidade de Ciberdefesa Nacional: *Contributos para a Definição de uma Estratégia Militar para o Ciberespaço*. Coleção "ARES", 36. Lisboa: Instituto Universitário Militar.

Nye, J. (2010). *Cyber power*. Belfer Center for Science and International Affairs, Harvard Kennedy School. https://www.belfercenter.org/publication/cyber-power

Palmer, Danny. (May 13, 2021). *Ransomware: How the NHS learned the lessons of WannaCry to protect hospitals from attack*. https://www.zdnet.com/article/ransomware-how-the-nhs-learned-the-lessons-of-wannacry-to-protect-hospitals-from-attack/

Richter, Felix. (November 15, 2022). *Amazon, Microsoft & Google Dominate Cloud Market*. https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/

Savolainen, Jukka. (November, 2019). *Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure – Weapons of Mass Disturbance (WMDi)?*. Retrieved from https://www.hybridcoe.fi/wp-content/uploads/2020/07/NEW_Working-paper_WMDivers_2019_rgb.pdf

Taylor, Petroc. (July 27, 2022). *Global market share held by operating systems for desktop PCs, from January 2013 to June 2022*. https://www.statista.com/statistics/218089/global-market-share-of-windows-7/

Zetter, Kim (March 3, 2016). *Inside the cunning, unprecedented hack of Ukraine's power grid*. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/