FEDERAL UNIVERSITY OF RIO GRANDE DO SUL
FACULTY OF ECONOMIC SCIENCES
GRADUATE PROGRAM IN INTERNATIONAL STRATEGIC STUDIES

BRUNA TOSO DE ALCÂNTARA

A COMPARATIVE STUDY ON CYBER POWER:
THE UNITED KINGDOM, FRANCE, AND GERMANY

Porto Alegre
2022

BRUNA TOSO DE ALCÂNTARA

A COMPARATIVE STUDY ON CYBER POWER: THE UNITED KINGDOM, FRANCE, AND GERMANY

Thesis submitted to the Graduate Program in International Strategic Studies of the Faculty of Economic Sciences at UFRGS as a partial requirement for obtaining the title of Doctor in International Strategic Studies.

Academic Advisor: Prof. Dr. Érico Esteves Duarte

Porto Alegre

2022

CIP - Catalogação na Publicação

Alcântara, Bruna Toso de
   A comparative study on cyber power: the United Kingdom, France, and Germany / Bruna Toso de Alcântara. -- 2022.
   225 f.
   Orientador: Érico Esteves Duarte.

   Tese (Doutorado) -- Universidade Federal do Rio Grande do Sul, Faculdade de Ciências Econômicas, Programa de Pós-Graduação em Estudos Estratégicos Internacionais, Porto Alegre, BR-RS, 2022.

   1. Power. 2. Cyberspace. 3. Germany. 4. France. 5. United Kingdom. I. Duarte, Érico Esteves, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

BRUNA TOSO DE ALCÂNTARA

A COMPARATIVE STUDY ON CYBER POWER:
THE UNITED KINGDOM, FRANCE, AND GERMANY

Thesis submitted to the Graduate Program in International Strategic Studies of the Faculty of Economic Sciences at UFRGS as a partial requirement for obtaining the title of Doctor in International Strategic Studies

Approved in: Porto Alegre, October 13, 2022.

EXAMINATION BOARD

____

Prof. Dr. Érico Esteves Duarte – Academic Advisor
UFRGS

____

Prof. Dr. Marco Aurélio Chaves Cepik
PPGEEI/UFRGS

____

Profa. Dra. Danielle Jacon Ayres Pinto
PPGRI/UFSM

____

Prof. Dr. Marcos Aurélio Guedes de Oliveira
PPGCP/UFPE

ACKNOWLEDGMENTS

First, I would like to thank the institutions that made this research possible: The Federal University of Rio Grande do Sul, which, through the Graduate Program in Strategic International Studies (PPGEEI), provided me with the structure and support necessary for the construction of this research; The Humboldt University zu Berlin, which allowed me a greater understanding of German's foreign and domestic policies; The Humboldt Institute for Internet and Society (HIIG), which, by granting me a fellowship, allowed me to get in touch with European interviewees, to expand my academic network and get insightful and helpful feedback on my initial research reasoning; and the Center of German and European Studies (CDEA), which by granting me scholarships to learn German helped me in my analysis and life while abroad in Berlin. I would also like to thank the Coordination for the Improvement of Higher Education Personnel, and the Research Support Foundation of the State of Rio Grande do Sul (CAPES/FAPERGS) for the scholarship granted to me, which partially financed this research.

Second, I would like to thank my advisor, Prof. Dr. Érico Esteves Duarte, who always encouraged me and gave me all the academic support necessary for developing this research. Similarly, I would like to thank Dr. Jörg Pohle, who was always very thoughtful and receptive to my research ideas, pushing me to further my academic goals. I would also like to thank all my academic peers who, directly or indirectly, helped me develop new perspectives. In particular, I thank Alexandra Paulus and Arthur Laudrain for their insightful feedback on my chapters on Germany and France, respectively, and Rodrigo Cardoso Silva, for some relevant comments on my conclusions and comparative analysis.

Third, I would like to thank all the interviewees of this research. I appreciate your time and wiliness to help me with my research.

Finally, I would like to thank my colleagues and manager, Carlos Francisco Cecconi, at the Brazilian Network Information Center (NIC.br), for their understanding and for granting me time to develop this research, and my mother, Rosane Beatriz Toso, for all her effort and advice at different stages of my life as a researcher.

ABSTRACT

This thesis aims to shed light on the concept of cyber power. Cyber power is a concept that has gained relevance with geopolitical dynamics reaching cyberspace and the increasing intertwining between the physical and digital. In this regard, this concept has been treated through three theoretical lenses: realism, liberalism, and constructivism. Still, constructivist approaches to the concept are sparse and deserve some attention. Thus, the thesis was based on a constructivist perspective, tackling the following research problem: How do states' perceptions of cybersecurity shape the form of their power projection? Does that confer a new form of power relations, therefore, cyber power as a phenomenon? To answer these questions, the research was developed to be a qualitative comparative study with a case center design. The selection of cases took a regional focus and encompassed conventional geopolitical European powers: the United Kingdom, France, and Germany. As auxiliary methods, the research used qualitative document analysis, practice tracing, and interviews to ensure robust findings. Specifically, the thesis was divided into seven chapters. The first chapter presents the research design and briefly contextualizes the debate over cyber power. The second chapter recalls what power means, going back to Political Sciences' influences on International Relations and the generational development of cyber power theories and indexes. The third, fourth, and fifth chapters focus on the case studies of the United Kingdom, France, and Germany, highlighting their digital mentalities (i.e., self and threat perceptions). The sixth chapter presents the comparison within the cases, pointing to similarities and differences in the concept of cyber power and how perspectives shaped the countries' international positions. The final chapter concludes the research findings and points out that strategic cybersecurity culture plays a relevant role in countries' cyber power perspectives. Even though cyber power was a term only used explicitly by the United Kingdom, it translated into the term sovereignty for France and Germany. In this regard, the idea of power in cyberspace presented itself as broader than just offensive and defensive capabilities, encompassing governance/diplomatic and economic/domestic affairs aspects. Besides, there is an influencing aspect, exposing that cyber power projection would be visible through diplomacy/cyber diplomacy.

Keywords: Power. Cyberspace. Germany. France. United Kingdom.

RESUMO

Esta tese tem como objetivo lançar luz sobre o conceito de poder cibernético. O poder cibernético é um conceito que ganhou relevância com a dinâmica geopolítica que atinge o ciberespaço e o crescente entrelaçamento entre o físico e o digital. Nesse sentido, esse conceito foi tratado por meio de três lentes teóricas: realismo, liberalismo e construtivismo. Ainda assim, as abordagens construtivistas do conceito são escassas e merecem alguma atenção. Dessa forma, a tese se baseou em uma perspectiva construtivista, abordando o seguinte problema: Como as percepções dos Estados sobre segurança cibernética moldam a forma de sua projeção de poder? Isso confere uma nova forma de relações de poder, portanto o poder cibernético como fenômeno? Para responder a estas questões, a pesquisa foi desenvolvida para ser um estudo qualitativo comparativo com um desenho centrado em casos. A seleção dos casos teve um enfoque regional e abrangeu potências geopolíticas europeias convencionais: Reino Unido, França e Alemanha. Como métodos auxiliares, a pesquisa utilizou análise qualitativa de documentos, rastreamento de práticas e entrevistas para garantir resultados robustos. Especificamente, a tese foi dividida em sete capítulos. O primeiro capítulo apresenta o desenho da pesquisa e contextualiza brevemente o debate sobre o poder cibernético. O segundo capítulo relembra o que significa poder, remontando às influências das Ciências Políticas nas Relações Internacionais e ao desenvolvimento geracional de teorias e índices de poder cibernético. O terceiro, quarto e quinto capítulos se concentram nos estudos de caso, do Reino Unido, França e Alemanha, destacando suas mentalidades digitais (ou seja, percepções de si mesmo e de ameaças). O sexto capítulo apresenta a comparação dentro dos casos, apontando semelhanças e diferenças no conceito de poder cibernético e como perspectivas moldaram as posições internacionais dos países. O capítulo final conclui os achados da pesquisa e aponta que a cultura de segurança estratégica desempenha um papel relevante nas perspectivas do poder cibernético dos países. Embora o poder cibernético seja um termo usado apenas explicitamente pelo Reino Unido, ele se traduziu no termo soberania para a França e a Alemanha. Nesse sentido, a ideia de poder no ciberespaço apresentou-se como mais ampla do que apenas capacidades ofensivas e defensivas, englobando aspectos de governança/diplomacia e econômico/ domésticos. Além disso, há um aspecto de influência no conceito, expondo que a projeção do poder cibernético seria visível por meio da diplomacia/ciberdiplomacia.

Palavras-Chave: Poder. Ciberespaço. Alemanha. França. Reino Unido.

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS[1]

AA – German Federal Foreign Office
ACD – Active Cyber Defence
AI – Artificial Intelligence
ANSSI – National Cybersecurity Agency
APT – Advanced Persistent Threat
ASEAN – Association of Southeast Asian Nations
BfV – Domestic Intelligence Service of the Federal Republic of Germany
BKA – Federal Criminal Police Office
BMBF– Federal Ministry of Education and Research
BMI – Federal Ministry of Interior and Community
BMVg – Federal Ministry of Defence
BND – Federal Intelligence Service of Germany
BSI – Federal Office for Information Security
CALID – Analysis Centre for Defensive Cyber Operations
CCB – Cyber Capacity Building
CCC – Chaos Computer Club
CERT – Computer Emergency Response Team
CESG – Communications-Electronics Security Group
CIA – Central Intelligence Agency
CIP – Critical Information Protection
CIR – Cyber and Information Domain Service
CISP – Cyber Security Information Sharing Partnership
CIT – Cyber and Information Technology
CMA – Computer Misuse Act
CNI – Critical National Infrastructure
CNO – Computer Network Operation
COMCYBER – Cyberdefense Command
CONTEST – Counter-Terrorism Strategy
COSSI – Operational Center for the Security of Information System
CPI – Cyber Power Index
CPNI – Center for the Protection of National Infrastructure
CSIS – Center for Strategic International Studies
CSOC – Cyber Security Operations Center
Cyber Agentur – Agency for Innovation in Cyber Security
Cyber-AZ – National Cyber Defence Centre
Cyber-SR – National Cyber Security Council
DCPP – Defence Cyber Protection Partnership
DCSSI – Central Directorate for the Security of Information Services
DGSE – General Directorate for External Security
DIME – Diplomacy, Information, Military, and Economic
DIMEFIL Diplomacy, Information, Military, Economic, Financial, Intelligence, Law Enforcement
DPR – Parliamentary Intelligence Delegation
DSD – Digital Strategy for Defence
DSTIL – Defence Science and Technology Laboratory

[1] The original acronyms when not in English have been translated, in case of translation I used either the official translation or own translation

EU – European Union
GCCS – Global Conference on Cyberspace
GCHQ Government Communications Headquarters
GDPR – General Data Protection Regulations
IA – Information Assurance
ICANN – Internet Corporation for Assigned Names and Numbers
ICT – Information and Communication Technology
IISS – International Institute for Strategic Studies
IoT – Internet of Things
IPA – Investigatory Powers Act
IR – International Relations
ISC – Intelligence and Security Committee
ISP – Internet Service Providers
ISS- Information Systems Security
IT – Information Technology
IT- SiG – IT Security Act
ITU – International Telecommunications Union
KdoCIR - Cyber and Information Domain Command
LID – Cyber Defense Policy
LIO – Cyber Offensive Military Doctrine
LPM – Military Planning Law
L2I – Cyber Influence Warfare Doctrine
MESRI – Ministry of Higher Education, Research and Innovation
MoD – Ministry of Defence
MoU – Memorandum of Understanding
NATO – North Atlantic Treaty Organization
NCF – National Cyber Force
NCPI – National Cyber Power Index
NCSC – National Cyber Security Centre
NCSS – National Cyber Security Strategy
NGO – Non-Governmental Organization
NIS - Network and Information Systems
NOCP – National Offensive Cyber Programme
NPSI – National Plan for the Protection of Information Infrastructure
NSA – National Security Agency
NSS – National Security Strategy
OCS – Office of Cyber Security
OECD – Organisation for Economic Co-operation and Development
OEWG – Open-Ended Working Group
OODA – Observation, Guidance, Decision, and Action
OSCE – Organization for Security and Co-operation in Europe
PIA – Future investments Program
PKGr – Parliamentary Control Body
PPC – Permanent Cyber Defense Posture
S&T – Science, and Technology
SCO – Shanghai Cooperation Organization
SDSR – Strategic Defence and Security Review
SGDSN – General Secretariat for National Defense
SGPI – General Secretariat for Investment
UK – United Kingdom

UN – United Nations
UNGGE – United Nations Group of Governmental Experts on advancing responsible state behavior in cyberspace in the context of international security
UP-BUND – Implementation Plan Federation
UP-KRITIS – Implementation Plan Critical Infrastructure
WSIS – World Summit on Information Society
ZfCh – Central Office for Encryption
ZITiS – Central Office for Information Technology in the Security Sector

INDEX

1 INTRODUCTION

To talk about power issues is to get into the heart of discussions in International Relations, and for that very reason, it becomes complex. This complexity comes from the flexibility and malleability of the concept of power itself and its various allocations and perceptions within the already-established theories of International Relations. However, this does not preclude its study but makes it increasingly necessary, especially in the face of new phenomena, such as those arising from relations between human beings and cyberspace.

It is valid to consider that the concept of power is not restricted to International Relations (IR). Given the evolution of IR's discipline, it absorbs many political scientists' positions, understandings, and perceptions. Thus, authors such as Dahl (1957, 1958), Bachrach and Baratz (1962; 1970), and Lukes (2005) are fundamental in the evolution of the concept of power and its use in political analysis, which after being absorbed, will be consolidated in theories, manifested in the Great IR Debates.

In this sense, cyber power emerges as an academic concept in the face of seemingly American demand for a better strategic understanding of cyberspace. Indeed, because cyberspace provides anonymity and stealthiness, this domain creates a new scenario for the state's power management. In other words, how to acquire, maintain and project cyber power is not yet fully understood. Thus, cyber stability comes into discussion.

If states project mistrust in cyberspace, a behavior similar to a security dilemma might emerge (GRIGSBY, 2017). State insecurity in the face of possible changes in their *status quo*, as a consequence of cyber power, could potentially lead to the replication of self-help behaviors, which could escalate to conflictive scenarios. The uniqueness of cyberspace as a common yet divided space poses challenges to states that involve working within different jurisdictions, balancing innovation and openness with security, and repurposing steady International Law mechanisms.

Amid this complex scenario, studies on cyber power have been developed. Still, little attention has been given to understanding how cyber power works empirically. Indexes such as the Belfer Center’s National Cyber Power Index 2020 seek to bring empirical elements in an effort to quantify cyber power, and sparse academic works such as the article of Knox (2018) on “The Effect of Cyberpower on Institutional Development in Norway,” use empirical analysis to track cyber power effects. However, cyber power as an emerging challenge displays a variety of not yet systematized data, making the complexities of cyber power use hidden (in what often remains as practices not openly disclosed). Therefore, one can say that analysis of cyber power use, especially in the international system, remains unexplored.

No unique theoretical proposal on cyber power accounts for the complexity of relations between the physical and the digital world since it crosses both the material and the immaterial part of the International System. Generations of cyber power theories have just been a few decades long, trying to catch up with the pace of the growing link between power and the digital domain.

Cyber power should be addressed as much as possible through approaches and disciplines (including International Relations) to fill that void. Given this need for understanding cyber power, analyzed here as a new phenomenon for IR, the following research problem guides the thesis: **How do states' perceptions of cybersecurity shape the form of their power projection? Does that confer a new form of power relations, therefore, cyber power as a phenomenon?** Thus, the general objective of this thesis is to identify what elements states perceive as cyber power and how this perception influences states' preference for security in cyberspace.

1.1 METHODOLOGY

To achieve the thesis objectives, a constructivist approach was taken. For constructivists, especially Wendt, the international system is what states make of it. In other words, the international structure is a social phenomenon since "it is impossible for structures to have effects apart from the attributes and interactions of agents" (WENDT, 1999, p.12). Interests and material power would have their effects and meanings dependent on the system's social structure, showing which of the three cultures of anarchy would be dominant (i.e., Hobbesian, Lockean, or Kantian). Thus, cyberspace is a medium created by human beings. It is also socially constructed, as its structure encompasses Information Communication Technologies (ICTs) that reach the globe, blending itself into the international structure and enabling systemic cyber power analysis.

This view of cyberspace as socially constructed, and subjected to systemic analysis, is not new. It can be found in the so-called Social Construction of Technology (SCoT), present in the philosophy of technology. Technology is considered not only technological artifacts (hardware) but also their use. For SCoT, technology is neither a neutral tool for problem-solving (i.e., instrumentalist view of technology) nor a value-laden force threatening human autonomy (deterministic view of technology). For SCoT, technology would be shaped and influenced by society and should be considered an expression of societal norms and expectations (CARR, 2016). Thus, “the starting point for SCOT perspectives in International Relations is the recognition that technology must be conceptualized as part of the international political system” (MCCARTHY, 2015, p. 33).

Therefore, this thesis innovates by seeking to identify not only the relationship between technology and power in International Relations. Technology may involve state response vectors beyond cyberspace – such as robotics, nano and biotechnology, and space systems, but in particular, how the concept of cyber power develops- centered on spheres of cybersecurity debate/ideas is still a pretty much-unexplored territory. It is expected to meet the demand for understanding this new type of power in the international structure so that states can project themselves, changing their status/relevance and meaning in the interactions with the other states.

It is important to highlight that the work does not follow constructivism's radical/social line. It maintains a constructivist ontological position based on positivist epistemological characteristics of conventional constructivism. According to Hopf (1998), this branch of constructivism seeks to present an alternative to the traditional international relations theory. It has a research program that conceptualizes threat equilibrium theory, the security dilemma, neoliberal cooperation theory, and democratic peace. Thus, conventional constructivism is not totally unconnected to the radical/critical variant of constructivism (e.g., concerning the denaturalization of the social world, the need to allocate data within a social context, the link between power and knowledge, and the mutual constitution between agent and structure) differs from it. Even though one expects to discover differences, identities, and multiple understandings, one assumes that it is possible to specify a set of conditions under which one can expect to see one identity or the other (HOPF, 1998, p. 183).

Thus, conventional constructivism accepts and even recognizes the need for contingent universalism. Therefore, it allows the adoption of positivist methods and epistemology (regarding sample characteristics, different methods, process tracing, and spurious verification). Even though this constructivist variant is not interested in traditional power relations, it is concerned with the production of new knowledge and insights from new understandings (HOPF, 1998, p.183). Cyber power is nothing more than a new understanding of power, as it presents itself as a new phenomenon characteristic of 21st-century society.

These characteristics allow dialogue with knowledge and initial attempts to develop a theory of cyber power, maintaining the idea of cumulative knowledge within a Lakatosian logic of positive heuristics. In this sense, cyber power can be considered a novel fact in lakatosian terms assuming the fact in question was not predicted by the best existing predecessor to the theory (i.e., methodological trait of novel facts) (GONZALEZ, 2001).

Moreover, by analyzing agents and structure as co-constituted, constructivism allows us to see how domestic issues resonate with the International System more comfortably. Even if it remains in anarchy, state interests are seen as conditioned on social practices involving variables such as identity, context, and culture (HOPF, 1998). This thesis was developed as a qualitative comparative study with a case centered-design using mixed methods to support conclusions. These methods included qualitative document analysis, practice processing, and semi-structured interviews.

Qualitative comparative studies allow one to find the most general patterns of a phenomenon in a higher degree of abstraction by exploring similarities and differences (TILLY, 1984). Moreover, comparative studies respond to the need to encompass the scope and deepen information by stimulating the development of new substantive theories (RAGIN, 1987), even though the control of variables is low. Indeed, according to Della Porta and Keating (2008, p. 202), "Although the quality of control of the variables is low in the comparative method, it is often the only method available for macro-dimensional, interdimensional, and institutional process studies."

The comparison made in this thesis was based on three case studies: the United Kingdom, France, and Germany. These countries were selected because they represent dominant narratives at regional and international levels regarding cyberspace and possess behaviors guided to power projection in the digital domain, but with variations between them.

In a survey conducted by European Council on Foreign Relations (ECFR) in 2018, the three countries were perceived as the most important security partners within the European Union (EU) (DENNISON; FRANKE; ZERKA, 2018, p.14). Additionally, all three countries were concerned about cyber attacks “either in terms of their likelihood, impact or manageability” and were widely seen as “leaders on cyber issues within the EU (DENNISON; FRANKE; ZERKA, 2018, p. 9). Even after Brexit, a new survey conducted by ECFR indicated that France and Germany remained the most influential countries within the EU, having "digital" among their top 10 policy priorities (PUGLIERIN; FRANKE, 2020).

On the behavior toward power in the digital domain, the UK presented itself as a pioneer in using the concept of cyber power for the first time in its 2022 National Cybersecurity Strategy (HMG, 2021b). France has also mentioned the idea of cyber power more clearly in its 2018 Strategic Review of Cyber Defense (SGDSN, 2018b). While Germany, in its turn, has demonstrated a growing will since 2016 to have a more significant presence in cyber policy, having as an action area to have an active role in European and international cyber security policy in its most recent National Cybersecurity Strategy (BMI, 2021). Thus, the regional relevance and the power-driven behavior toward cyberspace make the selected states a relevant sample to better link immaterial aspects to ideas of power in cyberspace. This allows, for instance, an in-depth look into perceptions in the cyber realm derived from traditional strategic security cultures.

At the international level, the selected countries also have great relevance. They participate in key cybersecurity policy forums, such as the United Nations Group of Governmental Experts on Advancing responsible State behavior in cyberspace (UNGGE) and the Open-ended Working Group on security of and in the use of information and communications technologies (OEWG). Moreover, the selected countries have explicit in their latest National Cyber Security Strategies their intent to have a more present role internationally (HMG, 2021b; BMI, 2021; PREMIER MINISTRE, 2015), having been ranked in the top ten cyber powers by National Cyber Power Index 2020 (VOO *et al.*, 2020). Also, the selected countries are an interesting starting point for researching cybersecurity cultures beyond traditional states' rivalry.

It is noteworthy that few cases allow the analysis to be more in-depth. According to Della Porta and Keating (2008, p. 205), seeking: an appreciative or esthetic explanation (i.e., an effort to understand principles by which the parties fit together), following an internal logic, that is, identifying actions for action – what led X to do Y? Besides, it avoided, with a small N, the stretching of the concept and the reliability in the degrees of comparison, that could promote a superficial analysis.

The data from the selected cases was gathered using a triangulation process involving mixed methods: Qualitative Document Analysis (QDA), Semi- Structured Interviews, and Practice Tracing. While QDA focused on pre-existing textual data, the interviews were designed to tackle critical issues in the literature review and the analyzed strategic documents. Practice tracing is a "methodological middle ground where patterns of meaningful action may be abstracted away from local contexts in the form of social mechanisms that can travel across cases" (POULIOT, 2015, p. 238). It focused on expanding contextual cybersecurity cultures from the cases to broader insights.

Specifically, the research started with a chronological analysis of published strategic documents of each case study, coding countries' self-perception and the perception of the other (threat), denominated in the thesis as digital mentality. Also, the study cases' strategic approach and material efforts (financial investment) on cybersecurity was coded in this first data set. The coding and data analysis was further crossed with secondary sources and some open-source speeches to gain validity. Besides, to complete a proper triangulation, answers from agency representatives collected from the application of semi-structured interviews were incorporated. The questions posed in the semi-structured interviews were based on initial data collection from a literature review and initial arguments based on a constructivist perspective. These arguments were the following:

a) State's perceptions of cyber power legitimize them to act strategically in the International System.
b) The concept of cyber power perceived by states generates a conception of hierarchy in the International System.
c) Cyber power is an autonomous element for states as its immaterial elements go beyond diplomacy and information and form a collective imaginary with an impact on the physical world.

It is essential to highlight that the interviews were made during the COVID-19 pandemic and were restricted to the reach and reply of digital communication (more details are in the memorial sub-section). From the initial coding of the individual study of cases, a comparison among the selected countries was made to observe common and diverging patterns within the set of categories applied (approach, self-perception, threats, investment). Also, some conclusions on countries' positions triggered by external cyber events were detailed, providing some practice patterns. In this regard, comparing cases allowed me to draw the findings on states' perceptions of the cyber power concept.

1.2 MEMORIAL

This thesis study started in 2018 with the first assessment of the literature review and the aim to gather interviews as a secondary data source within the countries selected. In 2019 I passed a one-year Fellowship at the Alexander von Humboldt Institute for Internet and Society (HIIG), where a primary task was to develop an international event bridging Brazil and Germany focused on cybersecurity. I would use the one-year time frame to gather my thesis interviews as a secondary task. The reasoning behind going to Germany was that from within Europe, it would be easier and feasible to travel to the other two countries and get the needed data.

Once in Germany, I pursue participation as an Erasmus student at the Humboldt University zu Berlin to better understand Germany's foreign policy. Thus, I took two disciplines at the University to help with my data assessment. Once the semester finished, the COVID-19 pandemic was set. The pandemic impacted my ability to travel within Europe, restricting networking and gathering potential interviewees. In the face of such an external event, I redesigned my strategy to reach potential interviewees from key agencies, using my University's email, emphasizing my credentials as a Brazilian Ph.D. candidate and HIIG fellow.

A few interviewees within Germany agreed to in-person interviews, while french and English interviewees agreed to conduct online interviewees, either providing oral or written questions. Since the topic was considered sensitive among the target agencies, six interviews were completed, relevant enough to support the information analyzed under QDA.

My engagement within HIIG also allowed me to present initial ideas (unfortunately before the conduction of the interviews) and receive some feedback from the researchers interested in the topic. The proposed event was concreted in 2020. It was named "Security in Cyberspace: dynamics, limits, and opportunities" and jointly organized by the Federal University of Rio Grande do Sul (UFRGS), the Federal University of Santa Catarina (UFSC), the São Paulo Law School of the Getulio Vargas Foundation (FGV-Direito SP) and the Alexander von Humboldt Institute for Internet and Society (HIIG). The event counted with a panel on power relations. Panel 04, titled "Interstate dynamics in Cyberspace and their consequences for International Relations balance of power," was fundamental to bringing me insights on coding the data I would be gathering.

Once I returned to Brazil in 2021, I was hired as a Technical Advisor at the Brazilian Internet Steering Committee, which allowed me to exchange ideas with researchers focused on Internet/Cyberspace issues. The exchanges were fundamental to the review of this work. Besides, some international experts in cyber issues, focusing on France, Germany, and the UK, agreed to review specific countries' sections, providing insightful feedback and a final presentation of the results, with the assessment of the interviews also made. The analysis, and thus thesis writing, was conducted between 2021-2022

1.3 CHAPTERS DESCRIPTION

The thesis is divided into four main blocks: Theoretical Background, Case Study individual analysis, Case Study Comparative Analysis, and Conclusion.

Chapter 2 sought to explain how Political Science and, further on, International Relations have dealt with the concept of power. Building on this explanation, the chapter further indicated how cyberspace studies had incorporated the concept of power and the gaps in the research agendas so far. Finally, the chapter exposed a new approach to understanding cyber power from a constructivist perspective.

Chapters 3, 4, and 5 sought to dive deep into the digital mentalities of the case studies countries (the United Kingdom, Germany, and France), focusing on the data gathered by QDA and the interviews. Therefore, the chapter looked beyond the countries' national cybersecurity strategies to identify the countries' perceptions and thoughts over cyberspace, cybersecurity, and cyber power over time. The concept of digital mentality was translated as the conjunction of ideas toward the cyber domain that reflects in the countries' self-perception and the perception of threats, considered the "other."

Chapter 6 is built upon the previous chapters, aiming to achieve two important goals. The first was to compare the case studies, highlighting common and different features between the UK, France, and Germany's digital mentalities. The second was to build upon comparisons, shedding light on the concept of cyber power itself and indicating broader inferences.

Finally, a conclusion follows, summarizing the thesis efforts and indicating the insights the research provided more clearly. Besides, it stressed gaps and opportunities for future studies.

2 CYBER POWER: A CHANGING RESEARCH AGENDA

The present chapter seeks to explain how Political Science and, further on, International Relations have dealt with the concept of power. Building on this explanation, the chapter further indicates how cyberspace studies have incorporated the concept of power and the gaps in the research agendas so far. Finally, the chapter exposes a new approach to understanding cyber power departing from a constructivist point of view.

2.1 THE CONCEPT OF POWER FOR POLITICAL SCIENCE AND INTERNATIONAL RELATIONS

The word power, etymologically, comes from the Vulgar Latin potere, substituted for the classical Latin posse, which is the contraction of potis esse, “to be able”; “authority” (FERREIRINHA; RAITZ, 2010, p. 369). In this sense, even if the concept originally had its essence on capacity/authority, its meaning has changed throughout history, proving adaptable to contexts and values. This malleability makes it a complex issue and “one of the most problematic in the field of international relations” (GILPIN, 1981, 13). Indeed, according to Lukes (2005a), the concept of power becomes problematic and controversial as other reference notions cannot elucidate its meaning, value assumptions cannot be disconnected from it, and its own contentedness matters in discursive sets.

Considering this scenario, tracking the change in power through human history, specifically in Political Science and International Relations debates, is necessary. These disciplines are relevant as they incorporate new elements to the concept over time, adding them into their discussions to understand human nature and the international system.

2.1.1 Power in Political Science: from one dimension to many

Power is an old concept used in Political Science that we can track at least since Ancient Greece, with Aristotle. In this sense, the idea of power has gone through many years of change and evolution. Still, for this study, since we want to grasp the spillover of Political Science into International Relations (IR) discipline, one can jump from the Ancient time to the Modern Age, when states were created.

In this regard, ideas toward power were attached to politics, closely related to the craft of governing. Thiscolese relation becomes apparent in the writing of classical political theorists, such as Hobbes, Locke, and Rousseau. However, a good example of power definition that translated into ideas of having a sort of control over others comes later on from the sociologist Max Weber, to whom the monopoly of the force was reserved to the state.

In this sense, Weber ties the circle of politics-struggle-power, a much more influential idea for International Relations, particularly security studies. For Weber, power (*Macht*) is "every chance within a social relationship to get your way, even against resistance, no matter what this opportunity is based on[2]." Derived from power, he develops the concept of domination rule (*Herrschaft*), which is "the chances for an order with a specific content to be obeyed by specified persons"[3] (WEBER, 1980, p. 28, own translation). As Guzzini (2017, p. 101-102) explains in, "Weber's scheme power is intrinsically related to the definition of "politics," where the differentiation of life chances (or: "selection," *Auslese*) in any social order is ultimately connected to the threat or use of physical violence and the competition to take control of it." Thus, if power imposes one's will over the other's, this would translate into struggle (Kampf), closing the vicious circle of violence and politics.

From Sociology back to Political Science, this influence was very present in the 1950s, which marked the start of the modern debate of power with Robert Dahl. Dahl was part of a pluralist branch of power scholars in Political Science[4], also influencing the first theories of International Relations. For Dahl, power is a relationship between individuals expressed in a symbiotic notation. Thus, the idea of power could be summarized in the following sentence: "A has power over B to the extent that he can get B to do something that B would not otherwise do" (DAHL, 1957, p. 202-3).

Such a relationship depends on four concrete power references:

a) Base, which would be the resources that can be exploited, such as the war potential of nations;
b) Means that would be the tools to use the resources, being a mediating activity between the bases of A and the answer of B,
c) Where the answer of B would be the scope; and
d) Amount, which could be translated via probability, giving the degree of relativization of power and conjugated with the scope and the means (DAHL, 1957, p. 203).

[2] From the original in German: "Macht bedeutet jede Chance, innerhalbeiner sozialen Beziehung den eigenen Willen auch gegen Widerstrebendurchzusetzen, gleichvielworaufdiese Chance beruht".

[3] From the original in German: "Herrschaft soll heissen die Chancen , für einen Befehl bestimmeten Innhalts bei angebbaren PersonenGehorsam zu finden".

[4] The pluralist branch within Political Science saw power as pluralistically distributed within the political system, especially the North American.

Furthermore, some requirements would be necessary to have a causal power relationship between A and B. Thus. A's actions must precede B's actions/responses; A and B must be connected in some way, and A's actions must successfully establish power relations over B (DAHL, 1957, p. 204).

In this way, power could only exist relatively. That is, A's power would exist in comparison to the power of B, being comparable in two ways: in the properties of the actors (i.e., bases and means) and the actors' responses (i.e., influence on scope, number of respondents, difference in odds change). Still, Dahl (1958, p. 466) states that only after "examining a series of concrete decisions" can power be analyzed. Therefore, what one should take into account are the decisions on issues in "key areas" that materialize in a conflictive way since it is a necessary, but not sufficient, condition that the key issue “should involve actual disagreement in preferences among two or more groups" (DAHL, 1958, p. 467).

Arguing that Dahl saw only "one face of power," Bachrach and Baratz (1962) inaugurate what is known as the second face of power within Political Science. For the authors, power, in addition to being contained in concrete decisions, would involve more abstract issues. According to the authors (BACHRACH; BARATZ, 1962, p. 948):

> Of course power is exercised when A participates in the making of decisions that affect B. But power is also exercised when A devotes his energies to creating or reinforcing social and political values and institutional practices that limit the scope of the political process to public consideration of only those issues which are comparatively innocuous to A.

Besides, Bachrach and Baratz (1962, p. 949) explain that political organizations have n intrinsic bias in “favor of the exploitation of some kinds of conflict and the suppression of others,” called “mobilization bias.” In this sense, the two sides of power must consider decision-making and non-decision-making. Thus, they explain that the second face of power would be further subdivided: in the successful use of power, that is, A guaranteeing the conformity of B, and in power as a guarantee of conformity through the threat of sanctions.

In this reasoning, Bachrach and Baratz (1970, p. 24-30) list a typology of power that would represent the forms of power in either of the two faces:

a) Coercion (A secures B’s compliance by the threat of deprivation where there is a conflict over values or course of action between A and B).
b) Influence (A, without resorting to either a tacit or an overt threat of severe deprivation, causes [B] to change his course of action).

c) Authority (B complies because he recognizes that [A's] command is reasonable in terms of his own values).
d) Manipulation (B agrees in the absence of recognition by part of it from the source or exact nature of the demand on it).

Looking for the map of typologies, the authors still alert that even if non-decision-making should be analyzed, it only manifests itself through the conflict of interests. In this sense, for them, the crucial thing would be to identify possible problems that non-decision-making prevents from being real (BACHRACH; BARATZ, 1970, p. 47).

In this sense, the position of Steven Lukes (2005b), regarding the presence, in the bi-dimensional notion of power, of a qualified critique on Dahl's proposal (with a behavioral focus) is valid. As Lukes (2005b, 25) explains, the bi-dimensional theory of power allows the consideration of ways that prevent decisions on potential issues (involving conflict of interests) from being made. Still, he goes further and presents the third face of power.

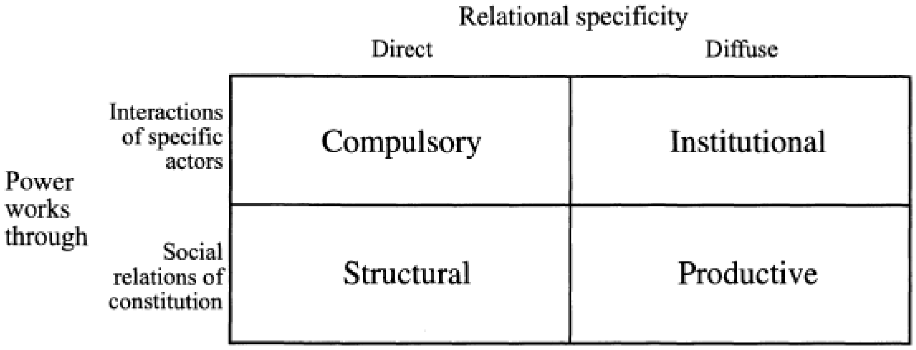
For Lukes (2005b), decision-making and control over the agenda would not necessarily occur through decisions. Potential issues should be considered as well as subjective and real interests, and there should be a focus on the observable (overt or covert) and latent conflict. In this sense, as Lukes (2005b, p. 28) put it, the three-dimensional view of power would involve a "thoroughgoing critique of the behavioural focus of the first two views as too individualistic and allows for consideration of the many ways in which potential issues are kept out of politics."

In this regard, Lukes (2005b, p. 37) defines the concept of power as "A exercises power over B when A affects B in a manner contrary to B's interests." He further explains that the three-dimensional view of power takes interests into a radical view, meaning power does not need to be active or intentional (LUKES, 2005a). For him, power "should remain attached to the agency that operates within and upon structures" (HAYWARD; LUKES, 2008, p.11). In other words, he understands that power operates upon and within society's structural features that allow actors to be powerful without exerting direct control.

In developing the power concept, other political scientists emerged after these three. Still, for this study, we will consider the proposals on faces of power as the seminal influential, leaving aside the explanation of other theorists, adding just one more contribution that spilled over IR (as we can see later in cyber studies). The contribution in question is from Barnett and Duvall.

Barnett and Duvall (2005) develop a concept of power that could be entangled in International Politics. In this sense, they can be interpreted as the missing link between the two disciplines (Political Science and International Relations), which could provide more answers to why their analysis influenced IR views on the matter. For the authors, power must be employed in multiple conceptions in a framework that encourages attention to power in its different forms. These multiple conceptions were translated into a taxonomy of their own involving power, encompassing: compulsory, institutional, structural, and productive power (See Table 1)

Table 1 - Barnett and Duvall's Power Taxonomy



		Relational specificity	
		Direct	Diffuse
Power works through	Interactions of specific actors	Compulsory	Institutional
	Social relations of constitution	Structural	Productive

Source: Barnett and Duvall (2005, p. 48).

Compulsory power refers to the direct control of an actor over the conditions of existence and/or the actions of another actor, not limited to material resources. It also implies symbolic and normative resources (example of Carr's distinction between military, economic, and propaganda power) (BARNETT; DUVALL, 2005, p. 49-50). In this sense, this form of power contemplates the vision of power for realists and neorealists.

Institutional power is the control actors indirectly exercise over others through diffuse interaction relationships. This power modality focuses on (1) formal and informal institutions that mediate A and B and (ii) the rules and procedures that define these institutions and guide and restrict the actions and conditions of existence of others. In this sense, there is an idea of dependence between agents and institutions. The ability to use the institution and the collective rewards are unevenly distributed in the future and go beyond the creators' intentions. (BARNETT; DUVALL, 2005, p. 51-52) Thus, this form of power contemplates the vision of institutionalists and neo-institutionalists.

Structural power is formed by the determination of capacities and social interests of the actors' capacities in a direct structural relationship with each other. It refers to the structure or co-constitutive relationships of structural positions that define the types of social actors. Furthermore, this form of power shapes the destinies and conditions of existence of actors in two ways: (i) Structural positions do not necessarily generate equal social privileges, as they allocate different capacities and advantages in relation to different positions, (ii) The social structure constitutes actors and their capacities, plus it shapes their self-understanding and subjective interests: it can prevent some actors from recognizing their own domination. In this sense, this modality of power is the most comprehensive for international relations, as it comprises structuralist theories, namely Marxism, neo-Marxism (world system), Constructivism (based on Wendt, mainly), and Realism (based on Machiavelli) (BARNETT; DUVALL, 2005, p. 52-55).

Finally, productive power works through diffuse constitutive relationships to produce the social capabilities of actors. It refers to discourse, social processes, and knowledge systems through which actors produce intentions and give meaning to their identities and capacities, constituting discourses as social relations of power. Thus, the analysis of productive power focuses on how diffuse and contingent social processes produce particular types of issues, fix meanings and categories, and create what is taken for granted and customary in world politics (BARNETT; DUVALL, 2005, p. 55-57). In this sense, this form of power approaches itself with constructivist ideas, meaning, less structural, and with some postmodern ideas that link power with knowledge à la Foucault.

In this context, the authors point out that such forms of power interact, relating the debate on the agent-structure duality insofar as the generic concern is with the relationship between the social context and human action. Thus, compulsory and institutional powers emphasize the agent and treat the structure as a constraint, while structural and productive powers emphasize structure in relation to the agent's purpose (BARNETT; DUVALL, 2005, p. 49). In the words of the authors:

> Any discussion of power in international politics, then, must include a consideration of how, why, and when some actors have "power over" others. Yet one also needs to consider the enduring structures and processes of global life that enable and constrain the ability of actors to shape their fates and their futures (BARNETT; DUVALL, 2005, p. 41).

The authors presented in this section (Weber, Dahl, Bachrach and Baratz, Lukes and Barnett, and Duvall) represent a glimpse into how the concept of power evolved throughout Political Science. Although this section did not thoroughly analyze the variations of the concept of power within Political Science, it made clear the complexation process of the concept itself over the years. Besides, it emphasized power understanding as a multidimensional phenomenon, making the point I would like to underline: the concept of power is highly flexible and capable of encompassing both material and immaterial elements. Indeed, with the proposal of Barnett and Duvall (2005), I already established some parallels with International Relations theories. However, much more from the font of Political Science was drained too, and developed along, International Relations, and the next section will broader this aspect.

2.1.2 Power in International Relations

Inspired by Weber, Hans Morgenthau understood that all politics is a power struggle. Therefore, the legitimate coercive power of the state, combined with a network of social norms and community ties, would distinguish domestic politics as an arena of potential progress. This Weberian thinking about power and Hobbesian thinking about the nature of man will serve as base models for the realism theory.

Therefore, for classical realists, international relations generally focus on power distribution among states. Agents would think and act in terms of interests, accumulating power via material capabilities. Power, in this sense, is seen "in terms of the material resources necessary to physically harm or coerce other states: in other words, to fight and win wars" (MINGST; ARREGUÍN-TOFT, 2017, p. 76). This thought would be translated into economic and military resources, considering population size and geographic aspects. Therefore, international relations would be a realm of necessity where states should seek power to survive in a competitive environment. In this regard, changes in the international and anarchic system should focus on the dynamics of the balance of power between states.

Despite being the pioneering theory, realists were not the only ones to vision power and its implications for the international arena. In International Relations, four major theoretical debates help us track international power. These debates were followed by debates within Political Science about power at the level of agents and national structures. In this sense, a discussion of the ideas of Dahl (1957, 1958), Bachrach and Baratz (1962; 1970), and Lukes (2005b) becomes an excellent roadmap to understanding how Political Science linked to theoretical debates on International Relations developed early perspectives on power.

In general, according to Lukes (2005b, p. 19), pluralists involve a behavioral focus in decision-making and on issues involving an observable conflict of interest. These interests are seen as expressed political preferences revealed through participation. Thus, considering that the debate in Political Science in the 1950s and 1960s was between behavioral and non-behavioral views of power, one can infer this debate also caught International Relations. The second major debate within the IR discipline was between behaviorists, such as Kaplan (1966), and traditionalists, such as Bull (1977).

This second debate focused on the relative merits of scientific investigation and historical methods for understanding international politics (i.e., materialism and philosophical realism). Behaviorists such as Kaplan (1966) celebrated the merits of statistical modeling and other quantitative methods for studying the causal laws of international relations. At the same time, traditionalists such as Bull championed the long-standing tradition of British scholarship that draws on political philosophy, law, and diplomatic history (BULL, 1977). The debate ended with an instrumentalist and positivist approach dominating the way we think about scientific research in IR.

In this sense, the conception of power underwent what Baldwin (2013) describes as an analytical revolution. Power began to be perceived as resources or capacities within a relational approach. The relational approach developed the idea of power as a type of causation (very much along the lines of Dahl, Bachrach, and Baratz). In this sense, the first face of power was seen anywhere, making policymakers in one country try to influence decision-making in another country. The second face, by its turn, would be illustrated whenever an agenda item is suppressed by some countries, despite the wishes of other countries (BALDWIN, 2013).

Perceiving power beyond concrete decisions and non-decisions and the agenda of states not necessarily materialized in conflicts, Lukes (2005b) goes through the area of values. The issue of values and structure would frame the third debate of International Relations: between the neorealists like Waltz and neo-institutionalists like Nye and Keohane. In this debate, the influence of institutions on the structures of the international system came to be more valued, and the plurality of actors involved in the international scenario came to be considered.

In fact, according to Baldwin (2013), an example of the third face of power in International Relations can be the supposed ability of the United States to get other countries to embrace the "Washington consensus" or "neoliberal economic visions." This third face of power is closely related to the concept of soft power from Nye (1990) and the idea of hegemony from Antonio Gramsci'.

For Nye (2011), soft power is the ability to affect others using co-opted means of agenda-setting, persuasion, and production of positive attraction to obtain preferred results. In contrast, hard power would be using force, payment, and some schedule adjustments based on them. Still, the author states that hard power and soft power sometimes reinforce or weaken each other, and good contextual intelligence is important to distinguish how they interact in different situations, hence the idea of smart power.

When explaining power, Nye (2011) models its behavior based on the faces of power. Thus, in the first face of power, which would induce others to do what they would not otherwise want, hard power would use force and reward to change B's existing strategies. Soft power would use attraction and persuasion. To change B's already existing preferences. In the second face of power, synthesized in structuring and setting the agenda, soft power would use the attraction or institutions for B to see the agenda as legitimate. At the same time, hard power would use force and reward to truncate B's agenda (B consented or not). Finally, in the third face of power, summarized in preference modeling, soft power would use attraction and/or institutions to shape B's initial preferences. Hard power would use force and reward to shape B's preferences.

For Gramsci, the question of hegemony, on the other hand, translates into a proletarian hegemony to replace the dominant bourgeois order through a permanent process of struggles and disputes of ideas capable of making the socialist project avenged. "Gramsci states that the supremacy of a social group or a class manifests itself in two different ways: domination (*dominio*) or coercion, and intellectual and moral leadership (*intelletualle e morale direzione*)" (FEMIA, 1987, p. 24). Gramsci's point of view considers that, in advanced capitalist countries, at the time of the consolidation of the bourgeois liberal order at the turn of the 19th to the 20th century, civil society would include complex institutions and mass organizations with active participation in their daily lives (COSTA, 2012). In other words, for Gramsci, “Hegemony is attained through the myriad ways in which the institutions of civil society operate to shape, directly or indirectly, the cognitive and affective structures whereby men perceive and evaluate problematic social reality” (FEMIA, 1987, p. 24). In this sense, for him, power is multidimensional, including material and immaterial elements.

The multidimensional perception of power becomes more evident in the debate between positivist and post-positivist theories of International Relations. In this context, power as a multifaceted phenomenon is partly perceived by placing the epistemology agenda of International Relations. This agenda presented post-positivist lines of ideas related to power under constructivist and Foucaultian visions.

Constructivists see the world as co-constituted, between agent and structure, giving much importance to the language since the International System is what states make of it. Wendt (1999, p. 97) divides International Relations theories into those that emphasize "brute material forces" as bases of power and those that see power as "constituted mainly by ideas and cultural contexts." For Wendt, despite some differences in the cognitivist, poststructuralist, and postmodern feminists, rule theorists, and structurationist, there is a shared concern with the sociological issue of identity and interest formation. Moreover, both modern and postmodern constructivists share a “cognitive, intersubjective conception of process in which identities and interests are endogenous to interaction, rather than a rationalist-behavioral one in which they are exogenous” (WENDT, 1992, p. 394). In this sense, Baldwin (2013) states that constructivists are part of the group with a more immaterial view of power.

According to Guzzini (2013), constructivist theories tend to understand power as related to agency and inter-subjective (including unintentional and impersonal power). In this sense, these theories are attuned to questions of open or taken-for-granted and "naturalized" legitimization processes. Thus, beyond an analytical approach to power (What is power), constructivists seek to conceptually understand the performative aspects of the concept (What makes power?), which, in turn, is incorporated into a history or genealogy concept (How did power come to mean and be able to do?) (GUZZINI, 2013, p. 217).

Hence the idea of meta-power presented by Singh. For Singh (2007, p. 49), “Meta-power goes beyond changes in preferences to examine changes in the underlying identities of international actors as well as changes in the identities of the issue-areas,” referring to the “changing epistemes of everyday life as a result of information networks” (SINGH, 2007, p. 50). For Singh (2007), meta-power would relate to constructivism, as instrumental power relates to liberal theory. In this sense, it would serve as a complementary element for a contextual understanding of the functioning of instrumental power. It recognizes that states continue to be important actors but operate in a widely changed cultural context in which neither security nor commerce can be understood in territorial and hierarchical terms.

This more cultural and immaterial idea follows a similar line within postmodern approaches having Foucault as a pivot. To Foucault (1979, p. 194), “(…) power produces; it produces reality; it produces domains of objects and rituals of truth”. This is not a distinct kind of power, one that is opposed to the power that “excludes,” “restrains,” or “hides.” His concept of power would be based on the Greek idea of Sumbolon, a dish in which two halves were broken (DEAN, 2017, p. 98). In this sense, for Foucault, power would operate from a relational web, functioning in the production of subjects, and through discipline, it (power) would generate and control.

By this influence, authors like Singh (2007), Sterling-Folker, and Shinko (2005, p. 637) discuss the similarities and differences between the realists' and postmodernists' thinking about power, stating that theoretical currents negatively characterize power. So while realists describe it as coercive and postmodernists describe it as disciplinary.

Expressly, postmodernists understand that control and struggle are relevant to conceptualizations of power. They manifested in two distinct but interrelated ways: physical and intellectual structures. The former include the institutions of governance, such as bureaucracies, while the latter are those that determine how we shape things and our knowledge of the world. This second sense of power emerges within Foucault's understanding of the relationship between power and the possibility of resisting structural domination. In other words, as power is conceptualized as fluid, reversible and non-linear (that is, as a network or network), it cannot resist structural constraints but (re)configure them (STERLING- FOLKER; SHINKO, 2005, p. 641). Therefore, resistance is a power resource that insists on being ad hoc.

Sterling-Folker and Shinko (2005, p. 642) point out that historical change occurs when structural fixity is replaced by acts of resistance, a form of power for postmodernists. Enloe's (1996) exposition on the marginalized voices explains this fact very well. Enloe (1996) explains that people on the margins do not have what it takes to affect international politics and the course of important events. Those who are silent do not have the "language of power." However, for the author, it is a mistake for researchers to leave them as an object of study of sciences other than international relations, as these marginalized voices can help explain international phenomena.

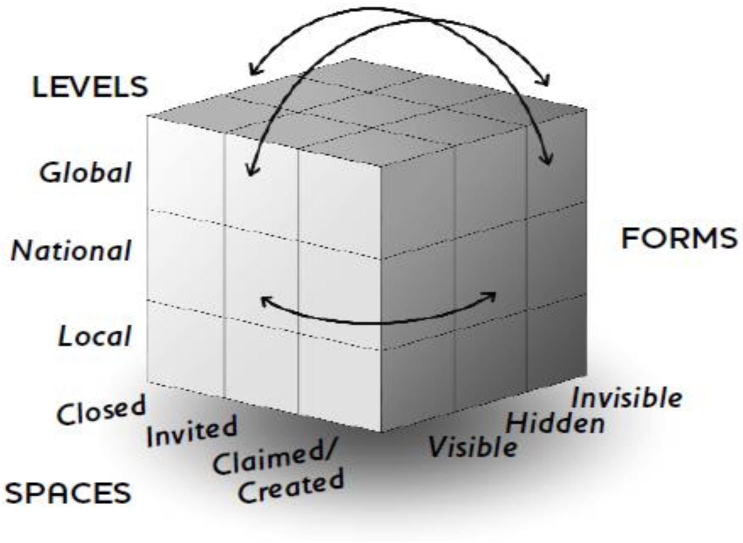
Therefore, Enloe (1996) shows that through the study of the marginalized, some evidence can emerge, indicating that the dominant discourse can cover up or (re)define as insignificant demonstrate important variables for establishing causal relationships. In this sense,

> It is only by delving deeper into any political system, listening more attentively at its margins, that we can accurately estimate the powers it has taken to provide the state with the apparent stability that has permitted its elite to presume to speak on behalf of a coherent whole in interstate trade bargaining sessions. Only with this explicit political accounting can we explain why the evolving international system takes the turns it does today (ENLOE, 1996, p. 200).

This thought of resistance and marginalized voices, in relation to the understanding of power, has gradually generated new proposals that are more inclusive of the concept, reinforcing the idea that power is multidimensional. In this sense, the idea of the cube of power by Gaventa (2006) (Figure 1) encompassing three dimensions between levels (local, national, global), spaces (closed spaces, by invitation and claimed), and forms (visible, hidden and invisible) is a suggestion pragmatic approach to studying power relations.

For Gaventa (2006), Dahl's maxim (A has power over B insofar as it can make B do something that B otherwise would not do) can be materialized by examining who participates, who wins, who loses, and which prevails in the decision-making process. On the other hand, expressed in the thought of Lukes, power is understood not only in terms of those who participate but also in terms of those who do not participate, which would be manifested in three ways: visible (referring to Dahl's concreteness), invisible (the relatively powerless internalize and accept their own condition and may not be aware of or act in their best interests) and hidden (keep issues off the agenda of decision-making arenas).

Figure 1 - The power cub: the levels, spaces and forms of power



Source: Gaventa (2006, p. 25).

As the author himself comments, the analytical proposal of power via a Rubik's Cube allows, as well as the game, innumerable combinations and, therefore, several possible power relations. Because of this, the interrelationship between these dimensions, while potentially opening up new opportunities and access to change, also poses enormous barriers for those seeking to challenge the status quo (GAVENTA, 2006).

The complex scenario put forward by Gaventa (2006) is captured in depth by Katzenstein and Seybert (2018, p.09), as they point out that the power question should not be constrained to control capacity distribution. For them, the fundamental question should instead be on, “how do power’s mechanisms define the (im)possible, the (im)probable, the unnatural, the normal.” Thus, they argue that power as either cause or effect (a trace we can observe in previous ideas displayed) does not coincide with political practice.

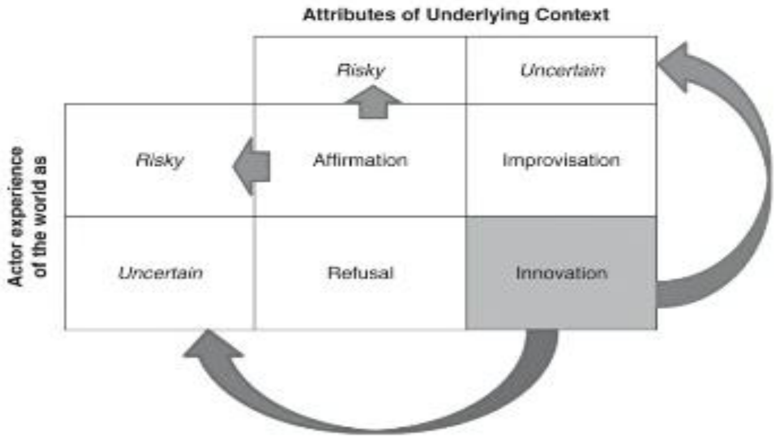
In this regard, Katzenstein and Seybert (2018) explain that power is analytically separate from practice as it affects the experience and context of risk and uncertainty. Thus, they propose to analyze the power question using the protean power concept.

Protean power refers to “the effect of provisional and innovative responses to uncertainty that rise from actor’s creativity and agility in response to uncertainty” (KATZENSTEIN; SEYBERT, 2018, p. 4). In this sense, they emphasize an aspect usually ignored by theory: uncertain scenarios. Therefore, protean power would better explain contexts of uncertainty, while the context of risks could be better understood in terms of control power, which seeks domination. In this regard, control and protean power would be competitive and complementary. They would be able to trigger a co-evolution and generate effects of diverse political practices involving either innovation, refusal, improvisation, or affirmation (in which affirmation may take the form of acquiescence or compliance) (see Figure 2).

The figure designed by the authors (Figure 2) focuses on “particular practices that relate actor experience and context attributes to power manifestations, and the degree to which the latter reinforce or undermine the different constellations of risk and uncertainty” (KATZENSTEIN; SEYBERT, 2018, p. 14). With this view Katzenstein and Seybert merge the ideas of “power over” (capability) and “power to,” or “power with” (capacity to actualize potentialities). This is so that even if an actor does not possess one of these types of power, he or she can own one of the others, indicating a feature of power reversibility. Thus, the authors advocate that the analysis of control and protean power politics can provide a broader notion of causality and protean power is better suited to explain open systems in which power operates in networks that are “extensive, loosely coupled and self-directed” (KATZENSTEIN; SEYBERT, 2018, p. 23).

All the explanations of power in this section incorporate power's complexity and multifaceted feature, including material and immaterial elements and the debate over agency and structure. Besides, they reinforce the idea that looking at the phenomenon is difficult. But to truly understand how these visions fit theoretical constraints, one must take a step back on the ontology of theories, particularly in this study related to International Relations. Even more, just with a clear-cut vision of ontology and epistemology, one can search for a better fit to explain power in cyberspace.

Figure 2 - Context, Experience, and Power



Source: Katzenstein and Seybert (2018, p. 13).

2.1.3 Ontological and epistemological views in International Relations and their implications for theory formulation

Discussions of power are reflected in International Relations' ontological and epistemological clash. After all, theories are still explanations about fragments of reality or the world as we see it. In this sense, they should be seen as “a tool for guiding actions, not a creed by which to live” (MCCARTHY, 2012, p. 24). In this sense, Della Porta and Keating (2008, p. 21) explain that within competitive approaches in the social sciences, there are discussions on three bases: ontological, epistemological, and methodological. The first is related to the existence of a real and objective world; The second is associated with the possibility of knowing this world and the forms that this knowledge would take; The third refers to the technical instruments used to acquire this knowledge. Furthermore, for the authors, there are four ontological and epistemological approaches within the Social Sciences: the positivists, the neo-positivists, the interpretivists, and the humanist.

For positivists, the world exists independently and subject to observation, being, in principle, knowable in its entirety. The researcher's task is to describe and analyze this reality from a distance, observing systematic rules and regularities that govern the object of study and are subject to empirical research. On the other hand, neo-positivists and post-positivists relax these assumptions, understanding that reality cannot be fully known; thus, causal relationships become probabilistic (DELLA PORTA; KEATING, 2008, p. 22-23).

Indeed, critical realists hold that “there is a real material world but that our knowledge of it is often socially conditioned and subject to challenge and reinterpretation” (DELLA PORTA; KEATING, 2008, p. 24). Similarly to social constructivists, who tend to hold that convenient ways of representing the world determine classifications. Thus, according to the authors, these approaches fall into an interpretivist framework. This framework understands the world as a series of interpretations or even within a more reflexivist framework. Within the reflexive turn, “social scientists’ interpretations feedback to the people through literature and media, influencing them yet again in what Giddens (1976) calls the ‘double hermeneutic” (DELLA PORTA; KEATING, 2008, p. 25).

Finally, humanists emphasize the individual even more. They understand that social science focuses on human behavior, which is always filtered by the subjective understandings of external reality by the people being studied and the researcher himself. In this sense, reality is not something tangible, and that is why the proposal of science must be the search for emphatic meaning (DELLA PORTA; KEATING, 2008, p. 25).

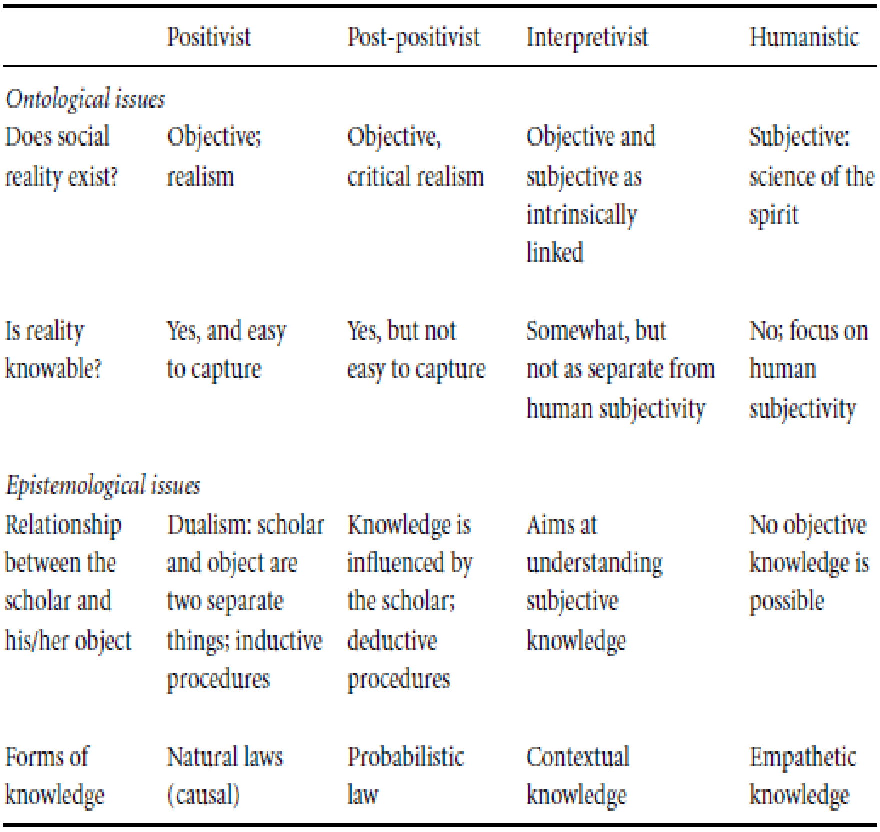
These approaches (see Table 2) are relevant because, as we saw in the previous session, the influence of Political Science on the concepts of power for International Relations, more broadly, has been debated since the second debate on International Relations. And this materialized in the cleavage in the theories of International Relations. In this sense, the discipline is “defined by its inclusiveness of competing approaches to methodology, although at times the perception that there is a certain methodological intolerance toward research that falls outside a particular tradition is also visible” (LAMONT, 2015, p. 17). Therefore, it usually lacks disciplinary cohesiveness, making analysis more challenging.

Therefore, the first major division of theories centers between those who seek to explain and those who seek to understand International Relations. Hollis and Smith (1991) elaborate on one of the first works concerning the issue, naming it the “two sides of the story.” They place on one side those who pursue empirical knowledge via a basis deriving from the natural sciences and those who follow empirical knowledge based on the natural sciences and seek to rely on more hermeneutical terms to understand empirical phenomena. They continue to discuss this separation using other adjectives: insiders or outsiders, causes versus meanings, and preferences versus rules, explaining that depending on the approach, the problem of levels of analysis can follow top-down or bottom-up patterns, which in turn will have repercussions in how agent and structure interactions take place in the international scenario.

According to Hollis and Smith (1991, p. 9), a schematization of the levels of analysis (i.e., International System, State, Bureaucracies, Individuals) presents three debates within the two choices of top-down and bottom-up patterns. Thus, in the first debate, a top-down approach makes the international system dominant, while a bottom-up approach is based on the sum of the actions of states. In the second debate, the top-down approach sees agents with their actions linked to rationality, while the bottom-up focus on bargaining between bureaucratic agencies. Finally, in the third debate, the top-down approach sees bureaucratic demands as shaping individual choices, while in the bottom-up, individual preferences will shape collective actions.

Jackson (2010, p. 9) observes that the implication of Hollis and Smith's empirical inquiry representation in IR "was that "scientists" did not have a monopoly on knowledge construction. There was an established, vibrant tradition operating with very different assumptions about how knowledge ought to be produced, and it was in some sense equal in value to its "scientific" alternative." After all, in all the great debates and within this inclusive IR discipline, we could not judge scientific theories from non-scientific ones as long as they followed ontological and methodological premises.

Table 2 - How many ontologies and epistemologies in the social sciences?



	Positivist	Post-positivist	Interpretivist	Humanistic
Ontological issues				
Does social reality exist?	Objective; realism	Objective, critical realism	Objective and subjective as intrinsically linked	Subjective: science of the spirit
Is reality knowable?	Yes, and easy to capture	Yes, but not easy to capture	Somewhat, but not as separate from human subjectivity	No; focus on human subjectivity
Epistemological issues				
Relationship between the scholar and his/her object	Dualism: scholar and object are two separate things; inductive procedures	Knowledge is influenced by the scholar; deductive procedures	Aims at understanding subjective knowledge	No objective knowledge is possible
Forms of knowledge	Natural laws (causal)	Probabilistic law	Contextual knowledge	Empathetic knowledge

Source: Della Porta and Keating (2008, p. 23).

The lack of consensus within the discipline (LAMONT, 2015) causes the various theories to be framed as empiricists. Following the basic positivist line with influences from

Popper[5], Kuhn[6] , and Lakatos[7]. The interpretivists, with a more abstract basis, focused on questioning ideas, norms, beliefs, and values that underlie international politics (See Table 3).

Given this cleavage, Jackson (2010, p. 16) warns us that IR scholars ignore that:

a) There is a normative aspect of the debates involving philosopher debates demarcating science from non-science
b) Philosophers involved in demarcation debates work in a transcendental mode
c) Lakatos' firm division between the methodological evaluation of a program and heuristic advice on what to do
d) The problem of demarcation can be considered spurious since “By simply taking what we like from the philosophical literature, we miss the context of, and the controversy surrounding, discussions about demarcation among philosophers.”

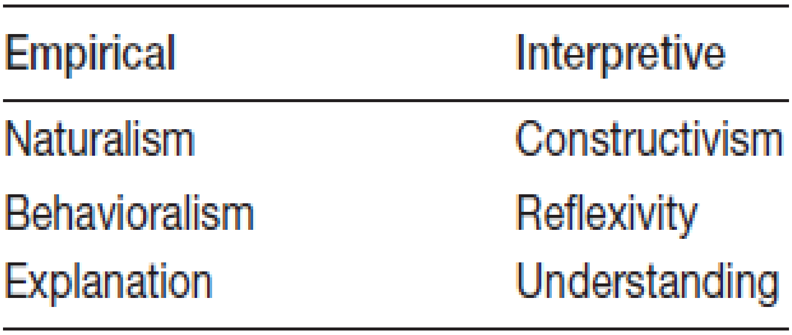
In this regard, Jackson proposes that knowledge should be goal-focused sought, considering science in Weberian terms. In other words, the necessary and jointly sufficient components of the science-knowledge question should be systematically related to its assumptions, capable of public criticism within the scientific community, and intended to produce worldly knowledge, whatever it is that the "world" may include. (JACKSON, 2010, p. 193).

[5] Popper had an evolutionary view of science and gave rise to what became known as the falsification theory. In the words of Jackson (2010, p. 13) “Popperian criterion revolves around the two behavioral implications of the falsifiability principle: researchers should be actively trying to falsify their conjectural claims, and only tentatively and provisionally accepting claims that survive a more or less rigorous series of tests; and researchers should abandon claims that have been falsified, because knowledge only expands if discredited propositions are discarded. Hence the focus of evaluation shifts from claims themselves (as long as they are falsifiable) to the behavior of the communities of researchers working with them, and science ceases to be a purely logical endeavor—it is, rather, a practical one”.

[6] Kuhn had an enormous influence on International Relations since his idea of paradigms allowed traditionalists to declare that they worked in different paradigms. At the same time, dissidents could portray themselves as heroes of a new paradigm (WIGHT, 2013). In summary, Kuhn states that “normal science” is “characterized by puzzle-solving, not by ongoing efforts to falsify any and all conjectures and claims” (JACKSON, 2010, p. 14). Thus, “normal science” would be characterized by consolidated paradigms. The development of science would only take place when the number of anomalies was so great that paradigms no longer supported them, creating a crisis (revolution in science) that would generate a new paradigm more appropriate. However, as Jackson (2010, p. 15) puts “Kuhn disrupts the very idea of “science” as a single unified field of endeavor, replacing that image with one of the islands of incommensurable research.”

[7] Lakatos proposes that analysts examine a series of statements in a “research program” to see if it progresses or degenerates over time In this sense, research programs could be on the rise or be degenerative – they would no longer explain reality but contain heuristics (a series of ontological and methodological rules and procedures) that could allow doing science (positives) or not (negatives). The construction of science would then be cumulative, as the research programs would be dynamic. After all, they would have a hardcore with premises, theories, and worldviews, but their protective belts would be full of premises that could be critical and remodeled. The research program would only be degenerative if the hardcore could no longer support criticism of the world's reality (JACKSON, 2010).

Table 3 - Empirical and Interpretive



Empirical	Interpretive
Naturalism	Constructivism
Behavioralism	Reflexivity
Explanation	Understanding

Source: Lamont (2015, p. 18).

Based on this knowledge logic, Jackson presents a different lexicon to understand commitments in philosophical ontology and the methodologies that arise from those commitments. Thus, he explains the idea of a mind-world dualism versus a mind-world monism and phenomenalism versus transfactualism. He places neopositivism and analyticism in the first group and reflexivity and critical realism in the second.

The mind-world dualism would be more realist since it separates the researcher from the world. The research is directed towards crossing the knowledge-production gap, aiming that the final valid knowledge be related to precise correspondence between empirical and theoretical prepositions on the one hand and the real character of a mind-independent world on the other. While the mind-world monolism is more idealist as it holds that research is part of the analyzed world. This ontology considered the world endogenous to social practices of knowledge production, including (but not limited to) academic practices. Therefore, the production of academic knowledge is not, in no sense, a simple description or record of already existing stable mundane objects. Regarding methodologies, phenomenalism treats knowledge as an organization of past experiences to forge valuable tools to investigate future (still unknown) situations. At the same time, transfactualism is about knowing things in-principle unobservables, focusing on grasping the deeper processes and factors that generate facts (JACKSON, 2010).

The division proposed by Jackson (2010) becomes objective when one considers what status knowledge has for the groups and how they understand the processes of analyzing their claims (Table 3). Thus, for positivists, validation occurs through testing, while analytics use narrative analysis. Critical realists use laboratory tests or transcendental arguments, and reflexivity theorizes the scientist's social conditions. This becomes relevant when evaluating theories because criticism can be appropriately addressed only if one can identify the theory’s bases, especially since it is known what the objective or type of knowledge a particular theory seeks.

In light of the previous explanation, two facts can be highlighted. The first one is that the concept of power differs in relation to its theoretical allocation. Theories come from different world perceptions and emerge from political thinkers with varying national/political power views. This will influence their conceptualization in different domains, such as cyberspace.

The second factor is that the concept of power varies in complexity. Relying upon the chosen epistemology, observable and unobservable elements can be taken differently. In this way, analyzing theories of power, particularly the conceptualized phenomenon of cyber power, requires the choice of a framework that includes diversity while allowing us to allocate theoretical choices within the lines of scientific thought of International Relations.

Therefore, for a proper evaluation of theories, the proposal by Buzan and Little (2000) seems a good fit. The authors propose to cross levels with analysis sectors in a matrix, adding sources of explanation to these crossings. For Buzan and Little (2000, p. 69), there are five levels of analysis in International relations: international systems, international subsystems, units, subunits, and individuals. International Systems comprise the entire planet, but according to the authors, there were more or less International Systems simultaneously, although disconnected. International subsystems are groups of units within the International System that can be distinguished from the whole by the nature or intensity of their interactions, which may or may not be regional. Units are entities composed of several subgroups, organizations, communities, and individuals, cohesive enough to be rational actors and independent enough to be distinguished from others and have a high position. Subunits represent organized groups of individuals within units capable of affecting the unit's behavior. Individuals are pointed to as most important in social science analyses.

Buzan and Little (2000) explain that these levels remain controversial in International Relations mainly because effects rely on which unit becomes the main focus of analysis. Also, validity depends on the looked system level, something we have already noticed in Hollis and Smith's (1991) statements. Notwithstanding, the sectors of analysis are new in the authors' proposal. Buzan and Little (2000, p.73) use these sectors as research facilitators, associating them with lenses that select a type of relationship and highlight the kind of unity, structure, and interaction associated with it. In this sense, they state that there are five possible sectors of analysis:

a) Military (encompassing relations of force of coercion and ability to fight wars, with the focus on the perceptions of the intentions of the actors among themselves);

b) Political (encompassing relations of authority, status, government and governance, recognition and concerns with organizational stability of the government system and the ideologies that give it legitimacy);

c) Economic (involving trade, production, and finance relationships, with a focus on how actors gain access to resources, finance, and markets necessary to sustain acceptable levels of well-being and political power);

d) Social (encompassing social and cultural relations, concerned with the collective identity, sustainability within acceptable conditions for evolution, patterns of language, culture, and religious and national identity)

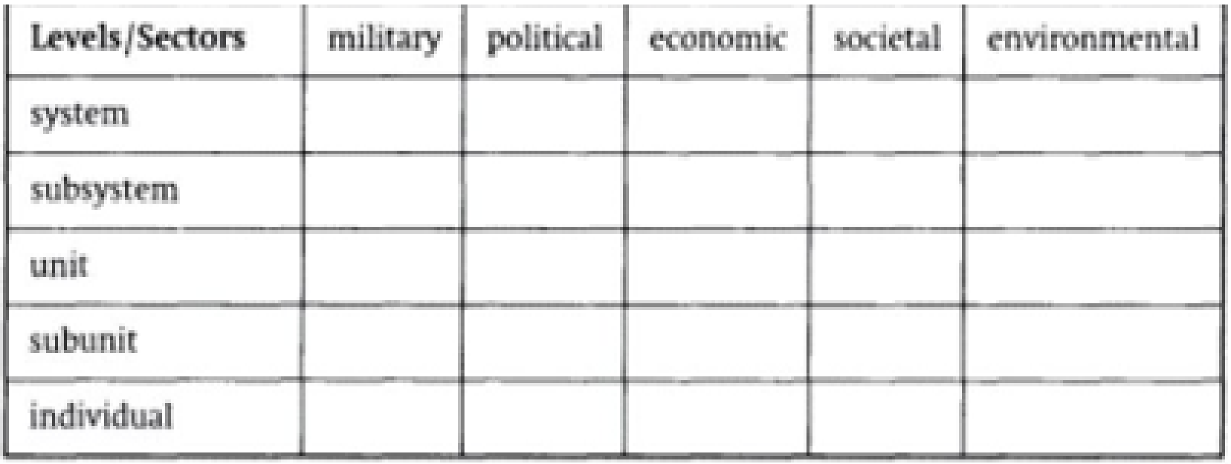
e) Environmental (related to human relations with the biosphere, focusing on disease transmission, global pollution, and movement of plants, people, and animals).

Finally, the sources of explanation would be behavioral explanatory variables that would be the key to the theory at any level of analysis or sector. According to Buzan and Little (2000), these sources of explanation can be of three types: process, capacity, or structure. The "process" source of explanation defines what units actually do and describes units' patterns of action and reaction conditioned by both the International System and the unit. The "interaction" source of explanation relates to the capacity which defines what units can do. In this sense, it can be about technological norms, rules, or shared institutions' capacities. Moreover, the type and intensity of interaction between units within the system or within units are depended on factors that mediate interaction capacity (i.e., geography, physical technologies, and social technologies). The “structure” source of explanation translates into the idea that the behavior of units is shaped by the environment in which they live, the focus on the principles by which structures are organized in the system, how they differ from each other, and how they appear in relation to each other one in terms of relative capabilities.

This way, a 5x5 matrix is formed (See Table 4). Still, Buzan and Little (2000) warn that using one sector while preserving clarity oversimplifies reality. At the same time, using many sectors risks complicating the image to the point of not being able to theorize. Despite the risks, using the matrix is interesting because it leaves mainstream perceptions. This is so because there is a functional differentiation between the units (they are functionally differentiated when one has differentiated and specialized elements of the function of a government) and structural differentiation (if the units have different or the same institutional arrangements).

Amid the explanation of this section, the next one will use the matrix proposal of Buzan and Little (2000) to assess the state of the literature on the theories proposed so far about cyber power.

Table 4 - Matrix of analysis levels and analysis sectors



Levels/Sectors	military	political	economic	societal	environmental
system					
subsystem					
unit					
subunit					
individual					

Source: Buzan and Little (2000, p. 77).

2.2 CYBER POWER THEORIES

Since cyberspace was consolidated after the advent of the Internet in the early 1970s, it is still too early to talk about well-developed theories about cyber power. However, this does not mean that no authors are repeatedly cited in academic works, much less that there are no works with diversified proposals. Thus, any analysis of this type of power arising from cyberspace must first consider the work of Tim Jordan (1999).

For sociologist Tim Jordan, cyber power is "the form of power that structures culture and politics in cyberspace and on the Internet" (JORDAN, 1999, p. 208). This power would not only cover issues of politics, culture, and authority but would be made up of three layers that would be interconnected: the first layer would be the individual, that is, power as possession of individuals, resulting in the cyber policy of greater access and defense of rights; the second layer would be the social one, involving the domination of power; the third layer would be the imaginary one, that is, power as a constituent of the social order (JORDAN, 1999).

The interconnection of these layers occurs through their relationships between actions and reactions, which feed each other. Thus, as the power at the base of individuals generates demands for new tools, other individuals with the capacity to manufacture them gain power and can manipulate those who do not have this capacity, creating interactions of domination that oscillate between an elite (i.e., from the techno-power) and society.

The dynamics of connection between the individual and social layers are guided by the "ceaseless process of individuals' struggling to make use of the vast resources of cyberspace in ways that then demand the renovation of cyberspace's substance by the few who wield the necessary expertise to remake the constituents of online life (JORDAN, 1999, p. 211-12). These two layers, moreover, are interconnected with the imaginary layer, as this layer would represent the collective imagination of cyberspace, its fears and hopes, and consequently, its identities (JORDAN, 1999).

Jordan (1999, p. 213) explains that the totality of cyber power would be these three levels and their connections. He further says, "Taken together they provide a complex map of the dominant structures and trends of life in cyberspace." However, this power would not point to total domination by either side (i.e., elite or individuals). In the words of Jordan (1999, p. 218):

> Cyberpower points not to the ultimate dominance of elites, though it clearly identifies the burgeoning power of elites, nor does it predict the libertarian ideal of individual empowerment, though it makes conspicuous the ongoing creation of powers for individuals in cyberspace. Cyberpower points to these processes continuing, driven by dreams and nightmares. When examining cyberpower we must always be aware of the roar of battle and the complex conflicts that define virtual lives, elites and dreams.

One can notice that Jordan (1999) opts for a bottom-up view using structure as an explanatory source, even though he refers to the social structure of cyberspace. In addition, he starts from a more reflexive perspective and, as a sociologist, uses the lens of the social sector, that is, part of an analysis of the individual and for the individual (i.e., society). In this sense, Jordan's (1999) effort is valid and relevant as cyberspace gives power to non-state actors. It does not serve as a good guide to power in cyberspace since its analysis becomes limited by focusing only on the immaterial aspects of cyberspace. After all, cyberspace [8] also encompasses physical structures, having a material component. Thus, in the face of a more positivist demand, for observable and concrete elements and the fear of an intertwining

[8] This study uses Libicki's definition of cyberspace. According to Libicki (2007), cyberspace is formed by layers involving physical, syntactic, semantic, and pragmatic layers. The first consists of the hardware part, i.e., processors, storage, switches, routers, telephones, and wired and wireless conduits. The second contains the programs and conventions by which information is formatted and by which systems are controlled and can be divided into sublayers such as the seven layers of the OSI Reference Model (Open System Interconnection). The third contains information maintained and manipulated by systems and transformation rules that manipulate knowledge in high-level applications. The last layer would deal with the purpose of a message/statement when considered in a particular context.

between the digital and physical domains in conflict scenarios, discussions of cyber power were directed into the realm of strategy.

2.2.1 The First Generation of Theorists: A Realist Ground

One of the first proponents of cyber power concept was Daniel Kuehl (2009). He is often cited in cyber power works and presents a realist approach to the issue. For Kuehl (2009, p. 28), cyberspace is perceived as a domain in which "whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies." Thus, he explains that the informational environment is composed of three dimensions: connectivity (Internet links that make the Web accessible to everyone), content (created and distributed digitally), and cognition (how communication and human interaction are affected by digital). Furthermore, cyberspace would shape and modify these three dimensions of the informational environment.

Based on this conception, Kuehl (2009, p. 38-39) understands that cyber power is a measure of the ability to use cyberspace. In this way, he conceptualizes cyber power as "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power." The author continues his thinking by saying that information is the closest element to cyber power. Thus, cyberspace and cyber power are dimensions of instruments of informational power under the PIME model (political, informational, military, and economic).

In this sense, cyber power increases economic strength by linking all agents together, increasing productivity, opening new markets, and allowing the administration of structures with an extensive reach. Likewise, cyber power increases military strength as cyberspace becomes an indispensable element of modern technology based on military capability. However, according to Kuehl, although present, it is less extensive in diplomatic and political fields (KUEHL, 2009, p. 39).

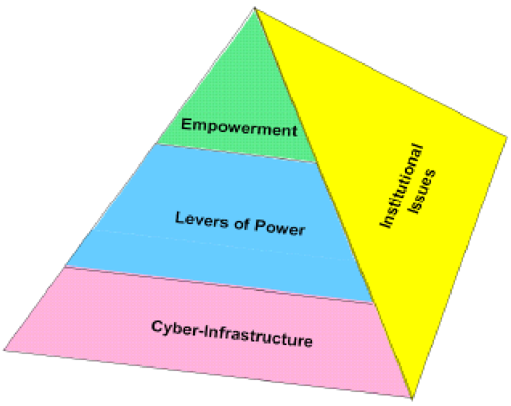
Thus, it can be seen that Kuehl (2009) works at the level of the unit (i.e., State) with a top-down approach, giving scope, within the PIME model, for a multisectoral analysis involving military, economic, political, and environmental sectors (i.e., informational). Like International Relations realists, he presents power as materially conceived from an objective reality and, therefore, subject to accumulation through economic and military means. In this sense, it is interesting that Kuehl's proposal mentions immaterial variables (political and diplomatic). However, it relegates them to the background as variables external to the causality of cyber power, thus disregarding the human and ideational element of cyberspace. Also, it should be noted that Kuehl (2009) gives a supportive role to cyber power, leading us to infer that the cyber domain serves as a conventional force multiplier, an idea stressed by the traditionalist stream within cybersecurity studies.

Based on Kuehl's (2009) idea of cyberspace, other authors have tried to develop material theories of cyber power, such as Starr (2009), Rattray (2009), Sheldon (2012), and Gray (2013). These theories focus much more on the issue of cyber operations as a resource to achieve power in the digital environment.

Starr (2009, p.21) seeks to develop an "evolving theory" of cyber power departing from a militarized and hierarchical view of power and proposing a pyramidal analysis model. As the author explains, the theory under construction is standardized and “patterned after the triangular framework that the military operations research community has employed to decompose the dimensions of traditional warfare.”

This triangular model (see Figure 3) has the cyber infrastructure in its lowest layer, comprising components, systems, and systems of cyber systems. The second layer includes the power levels within the D/PIME logic (i.e., political, diplomatic, informational, military, and economic). Finally, the last layer, supported by the infrastructure and power levels, generates the basis for empowering the entities at the top. Still, in this model, the author suggests that each level is affected by institutional factors. These factors include “governance, legal considerations, regulation, information sharing, and civil liberties considerations” (STARR, 2009, p. 22).

Figure 3 - Broad Conceptual Framework



Source: Starr (2009, p. 21).

Besides, Starr (2009, p. 22) points out that cyber power and cyber strategy are complementary terms. This is so because he considers cyber strategy "the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational domains." In this sense, Starr emphasizes that one of the critical issues associated with cyber strategy "deals with the challenge of devising "tailored" deterrence" to affect the behavior of the critical entities empowered by developments in cyberspace."

Interestingly, Starr (2009) explains he only developed the military and informational side in his “theory.” In this way, and observing studies with a tendency to evaluate methods of efficiency of cyber operations, he concludes that a theory of cyber power should involve four key factors:

a) Technological advances

b) Speed and scope of operations

c) Characteristics control and

d) National mobilization

Technological advances refer to technological dependence, which brings new strategic vulnerabilities since the diffusion of these technologies and the technological advances themselves, added to the low cost of entry, increase the power of non-state agents. On the other hand, the speed and scope of operations bring the element of control and command automation and the speed that the OODA cycle (i.e., Observation, Guidance, Decision, and Action) can reach. This automation and the OODA process can lead to a mismatch between virtual actions and human reactions or even human perceptions (STARR, 2009).

As for the control of characteristics, he refers to the defense of cyber hotels, where technology and communication systems are concentrated (referring to Mahan's idea of chokepoints) since they can change quickly in the cyber environment. On the other hand, national mobilization refers to the need for readiness. This would require a link with the private sector (given that much of the physical infrastructure of cyberspace is linked to this sector of society) in addition to the development of a cyber career and the creation of a reserve of reservists for eventual national needs for access to intellectual capital (STARR, 2009).

In addition to these statements, Starr (2009) develops, from an informational point of view, ideas of influence operations from a strategic and tactical perspective. In this sense, it generates an approach to link operational objectives and processes to the Doctrine of Organization, Training, Material, Leadership, Education, Personnel, and Facilities requirements. This doctrine has strategical, operational, and tactical levels. The strategic level focuses on ensuring resilience in support of critical infrastructure. The operational seeks to create a capable opposing force. The tactical focus is on placing a high priority on ensuring information. Thus, the author ends by indicating that developments in cyberspace could substantially affect future efforts to improve influence operations (ex, implement precision-guided messaging).

Thus, it can be seen that Starr (2009) also adopts a top-down approach, focusing on the unit, while the level of analysis bases its explanation on the capabilities of interactions and approaches the subject with a neorealist bias. In this way, Starr is also tied to material factors. Even though he considers immaterial variables in more significant weight, at least more than Kuehl (2009), the author does not explore them. Neither sees them as variables external to the main causal analysis (e.g., OODA cycle), making a limited analysis of possible power relations in cyberspace.

As Cavelty (2018, p. 4) points out, these early US cyber power theorists have a more state-centric view of cyber power, thus prioritizing top-down approaches and pointing to supporting strategic elements (i.e., cyber strategy and national security for cyberspace). Furthermore, both recognize that the presence of non-state actors materializes, but "Nonstate actors appear as passive ‘intellectual capital’ needed in all theory elements, whereby the state is the political entity that needs to learn how to optimize its cyber power."

Following a more strategic line, Rattray (2009, p. 257) considers cyber power a fundamental enabler for the full range of instruments of power. To the author, “The challenge of managing the technological foundations of cyberspace means that human capital is a fundamental influence on the use of this environment.” Thus, he parallels the idea of power from other domains (land, air, sea, and space) to find common characteristics for constructing an environmental theory of cyber power.

As for land power, Rattray (2009, p. 258) takes up Mackinder and Spykman's ideas about the importance of Heartland[9] and Rimland[10]. He concludes, "Just as Mackinder and Spykman did for land power, those who would develop a theory of cyber power must

[9] For Makinder, the Heartland would be located in central Eurasia. It would extend from the Volga to the Yangtze and the Himalayas to the Arctic. Thus, disputes over the control of the Heartland would be at the center of global geopolitics, as the state that controlled the entire Heartland could try to obtain outlets to the open sea and become an amphibious power that could dominate what it called the territory of the World Island. The Island of the World refers to Eurasia and North Africa, connected by the Ural Mountains and the Isthmus of Suez. In this way, dominating the Island of the World, a State would decide the direction of world politics.

[10] For Spykman, geopolitics is planning a country's security policy in terms of its geographical factors. Thus, he criticized Mackinder for overestimating the Heartland as of immense strategic importance due to its vast size, central geographic location, and supremacy of land power rather than sea power. Therefore, for Spykman, the Rimland, which would comprise the strip of coastal land that surrounds Eurasia, would be more important than the Central Asian zone (i.e., Heartland) to control the Eurasian continent.

determine the key resources and focal points for transit in cyberspace." While concerning maritime power Rattray (2009, p. 258-9) turns to Mahan and Corbett, explaining their respective ideas of chokepoints[11] and fleet in being[12], to demonstrate that the theory of maritime power explicitly deals with how it is central to the environment the global maneuver and impact of technological change. In the author's words:

> For example, much of cyberspace relies on fiber optic cables that transit the seabed; these cables and associated facilities may constitute new chokepoints. Alternative routes will exist in cyberspace, such as satellites for intercontinental connectivity, but these alternatives, too, might be potential chokepoints. As such, each offers a potential locus of national control (RATTRAY, 2009, p. 259-260).

As for airpower, Rattray (2009) takes up the ideas of Mitchell, Douhet, and Trenchard that the plane could have greater precision and impact when reaching strategic points to shake not only the resources but also the enemy's morale (i.e., strategic bombing).In addition, he considered the question posed by Douhet that air warfare would not admit defense, only offense. Based on these ideas, Rattray (2009) states that, as in the 20th century, questions such as the meaning of offensive-defensive interaction, the impact of this new type of power on the domestic budget, the cooperative possibilities and limitations around the security of the new domain (aerial), now turn to cyberspace.

Finally, concerning space power, Rattray (2009, p. 261) states that researchers such as Colin Gray and Geoffrey Sloan, in 1999, already warned about the strategic challenges involving the Earth, moon, and solar spaces. “They stressed the strategic significance of locations in space,” as the spaces involving geographic synchronicity of rotations and gravitational attraction. Furthermore, he cites Harter, for whom space will significantly improve the ability of friendly forces to strike enemy centers of gravity, paralyzing the adversary so that the other domains of warfare (land, air, sea) can gain superiority in the war theater. In this sense, and agreeing with Harter that there is a dependence on space to transport information globally and network operations that use space systems, Rattray (2009, p. 262) states that space satellites and orbital locations become bottlenecks in the cyber world.

Given these links, Rattray (2009) perceived four characteristics common to the domains, the same ones that Starr (2009) had listed, that is

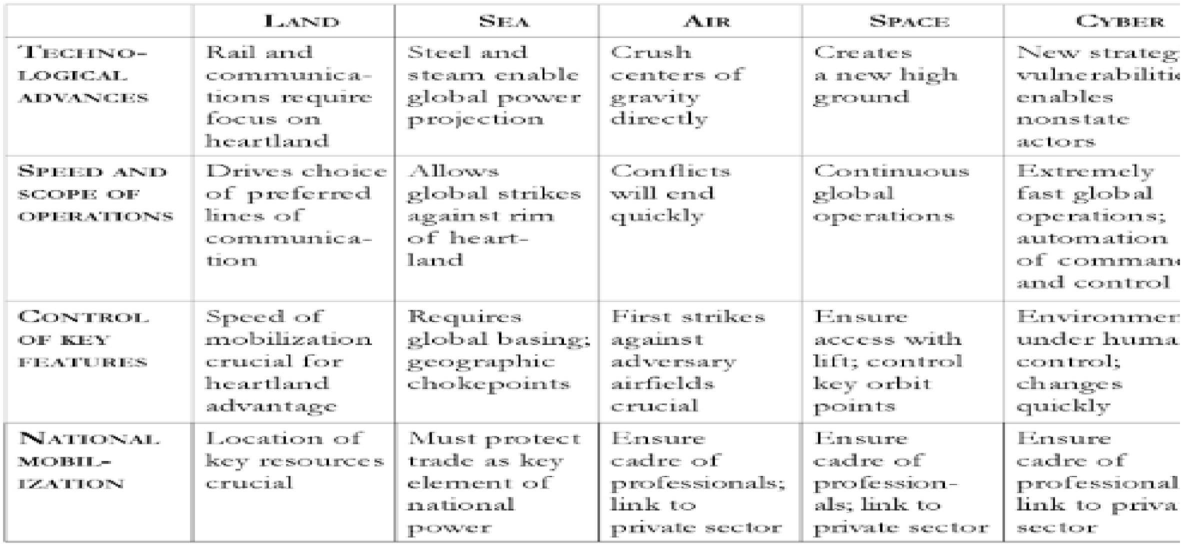
[11] In "The Influence of Sea Power on History," Mahan reviewed the role of sea power in the rise and growth of the British Empire. He described the sea as a "great highway" and "wide common," identifying several narrow passages or strategic "chokepoints," whose control contributed to Britain's command of the seas (SEMPA, 2014).

[12]“Corbett emphasized the superiority of defense and dispersion of forces in naval war and insisted on the significance of silent pressure using the navy’s presence, like the “fleet in being,” a strategy to temporarily disperse and avoid the enemy’s forces” (SEKINE, 2012).

a) Technological advances,
b) Speed and scope of operations,
c) Control of characteristics control and
d) National mobilization.

However, Rattray (2009) further characterizes each dimension (Table 5).

Table 5 - Elements with the Cyber Environment Compared with Other Environments



	LAND	SEA	AIR	SPACE	CYBER
TECHNOLOGICAL ADVANCES	Rail and communications require focus on heartland	Steel and steam enable global power projection	Crush centers of gravity directly	Creates a new high ground	New strateg vulnerabiliti enables nonstate actors
SPEED AND SCOPE OF OPERATIONS	Drives choice of preferred lines of communication	Allows global strikes against rim of heartland	Conflicts will end quickly	Continuous global operations	Extremely fast global operations; automation of comman and control
CONTROL OF KEY FEATURES	Speed of mobilization crucial for heartland advantage	Requires global basing; geographic chokepoints	First strikes against adversary airfields crucial	Ensure access with lift; control key orbit points	Environmer under huma control; changes quickly
NATIONAL MOBILIZATION	Location of key resources crucial	Must protect trade as key element of national power	Ensure cadre of professionals; link to private sector	Ensure cadre of professionals; link to private sector	Ensure cadre of professional link to priva sector

Source: Rattray (2009, p. 273).

In this way, to gain an advantage in the competition within cyberspace, the ability to assess trade-offs related to operational values, connectivity costs, vulnerabilities, and threats, can strike the balance of effectiveness (RATTRAY, 2009). On the one hand, a "robust, defensible infrastructure will depend on shaping the technologies employed, the obligations of operators of key networks and infrastructures, and the ability to coordinate government-private sector investment and responses to attacks" (RATTRAY, 2009, p. 273). On the other hand, resource mobilization would require leadership strategies, requiring both decision-making processes and the adoption of rules, amid a changing environment aimed at external networks and mission partners that balance usability and security (RATTRAY, 2009).

Thus, Rattray (2009) also follows a top-down approach, focusing on the level of analysis of the unit. Furthermore, he brings the structure as an explanatory force: the cyber environment as a domain of war. However, his vision remains material and realistic, including the human variable as a resource / technical capacity, disregarding the immaterial field of cyberspace.

For Sheldon (2012, p. 211), cyberspace is the domain in which cyber operations take place, and cyber power "is the sum of strategic effects generated by cyber operations in and from cyberspace." Thus, it is relevant to understand the strategic context of cyber power, which serves both peacetime and wartime. According to Sheldon (2012, p. 210), "Cyber power can be used in peacetime and war because it is stealthy and covert, it is relatively cheap, and its use favors the offense but is difficult to attribute to the perpetrator."

In addition, cyber power for Sheldon (2012) would be different because cyberspace has its characteristics. In other words, cyberspace: depends on the electromagnetic spectrum; requires human-made objects to exist; can be constantly replicated; has a relatively low cost of entry; offensive operations are dominant (i.e., the offense has an advantage); it has four layers (infrastructure, physics, syntactic and semantic), He further explains that the control of one layer of cyberspace does not mean the control of the others, it ends up influencing the possible operations and strategies, which will accumulate in cyber power. He adds that these cyberspace singularities reflect cyber power.

Therefore, cyber power would end up being:

a) Omnipresent (it is everywhere, having absolute and simultaneous effects in other domains),

b) Indirect (generates limited coercion), and

c) Stealthy (causes non-attribution/anonymity problem).

In this sense, Sheldon (2012, p. 216) explains that although the coercive value of cyber power is still “proving its worth,” its capabilities generate real strategic value, and due to its characteristics, it ends up becoming an offensive instrument. In fact, according to Sheldon (2012, p. 217-18), cyber power will feature prominently in future wars. Thus, “victory will favor the side able to effectively command forces deprived of information while simultaneously using cyber power to deceive, deny, demoralize, and disrupt enemies, thus compromising their ability to comprehend the strategic environment.”

Moreover, he criticizes Rattray's work in “Strategic Warfare in Cyberspace” for emphasizing technological and organizational dimensions at the expense of pertinent elements and focusing exclusively on an analogy with air power. Sheldon (2012) also criticizes Starr for digressing at the operational and tactical levels, failing to relate cyber power to the political and strategic context.

Thus, it is clear that Sheldon (2012) also has a top-down approach, characterizing the importance of the strategic, operational, and tactical fields. However, even though he brings the contextual variable to the analysis, he maintains the material economic (i.e., private sector) and military (i.e., offensive resource) focus of cyber power, considering it, although unique, one more tool at the service of the State (SHELDON, 2012, p. 209).

Gray (2013) also emphasizes the strategic issue but focuses more on the context of geography and information. For this author, the strategic understanding of the cyber environment focuses on three elements: a general theory of strategy, geography (explaining that cyberspace has a distinct geography and domain), and information (what connected networks of computers can do when passing information, and which are the consequences).

Based on this basis Gray (2013, p. 54) explains that the framing of cyberspace as a domain of war is necessary. However, "its nonphysicality compels that cyber should be treated as an enabler of joint action, rather than as an agent of military action capable of behaving independently for useful coercive strategic effect." This leads to understanding cyber power as more useful if instrumentalized as a facilitator of joint military operations. Thus, this type of power would be one of the many ways to collect, store, and transmit information (GRAY, 2013).

For Gray (2013), cyber power should be understood as another weapon category within a general strategy theory. A weapon, for him, must be understood as something used to cause damage. However, the author defends the thesis that the sky is not falling. The greater damage to the nation (i.e., the USA) will not happen due to cyber activity per se. This is because cyberspace would have a secondary role in the physical effort of war/conflict. Besides, although difficult, the defense could be effective enough. While intelligence is an important aspect of cyberspace, information should not be overemphasized.

Thus, what is noticeable in Gray (2013) is his perspective of cyber power, which is also offensive. But unlike Sheldon (2012), cyber power would not be unique and linked to conventional capabilities given its immaterial part. In other words, even though Gray (2013) recognizes the immateriality of cyberspace, he relegates it to a secondary plane. In this way, he proceeds with a top-down proposal at the unit level, with an explanatory focus on the capacity for interaction and positioning cyber power in a supportive role for state strategies.

It is interesting to note that from 2011 onwards, several theoretical proposals of cyber power entered the strategic field (perhaps reinvigorated by the discovery in 2010 of the Stuxnet virus), with a realist traditional view of power, but with some variations between them. These visions will generally be based on military dynamics, conflict contexts, and analogies with powers from other war domains (land, air, sea) and/or classical strategists of these domains.

Bonner (2011), for example, focuses his analysis of cyber power on joint military campaigns. For him, the value of cyber power in this context is given as a source of cohesion, guidelines, and a tool that allows military forces to classify, correlate and assimilate large amounts of information. Thus, elaborating on the possibilities of cyber power, he draws parallels with elements of land power (land use and fortifications), sea power (dissimulation, persistence, and intelligence), and air power (speed, mobility, and intelligence).

Still, Bonner (2011, p.116) illustrates his points with events in Estonia in 2007 and Georgia in 2008. Affirming that cyber power would have force as a coercive tool, at least at the operational level of war, "especially in achieving cyber superiority when defending retains dormant cyber power capabilities."

Like Bonner (2011), but focused on technical-human and economic capabilities, Klimburg (2011) develops an Integrated Capabilities Model. This model divides a state's cyber power into three dimensions:

a) Ability to coordinate government action,

b) Ability to collaborate with international partners, and

c) Ability to coordinate with the non-state sector.

In this model, Klimburg (2011), despite considering non-state actors, maintains a state-centric view since there is the assumption that even if non-state actors carry out independent actions, the state can be the biggest beneficiary. In the author’s words:

> Computer-network exploitation attacks can require considerable resources, and many observers believe that the more sophisticated attacks could only be undertaken by state actors. There are, however, indications that even highly advanced espionage attacks, requiring hundreds of hours of programming and with a clear political focus, are being executed by non-state actors, albeit for the benefit of a state (KLIMBURG, 2011, p. 43).

Thus, the model proposes attention to political actions that integrate the State with non-state actors, specifically the private sector and civil society, since a large part of a State's cyber capabilities is outside the direct control of the government, situated precisely in these fields.

In this same economic logic, Barcomb (2013, p. 81) also falls into materialism when focusing on protecting economic interests that a parallel with the maritime domain can offer. For the author, power in the digital sphere would be the ability to decide what is important and what is not on the Internet, bringing the flow of information closer to lines of strategic communication with economic impact. Thus, he indicates that strategies in cyberspace should be centered on relations of construction, performance, and legitimacy that would be more effective than those based on force (BARCOMB, 2013).

Another relevant author is Tabansky (2016), who, within an economic-military logic, in his article "Towards a Theory of Cyber Power: The Israeli Experience with 'Innovation and Strategy," elaborates an interdisciplinary cyber analytical framework, using as a study the Israel case. For the author, cyber power would act as both an instrument and a tool. It would depend on the context, perception, and anticipation of the relationships involved. Whereas strategy would be to get more out of a situation than the initial balance of power would suggest (i.e., the art of creating power).

For Tabansky (2016, p. 62), the missing ingredient in cyber power scholarship and policy is strategy, and “a democracy seeking cyber power should optimally engage in an iterative strategic process loop.” This optimization would take place via four processes. The first is reassessing a specific national strategy to clarify the desired ends. Second, understanding cyber means design, meaning the feasible ways they serve the defined strategic ends, focusing on non-military aspects, innovation, and soft power. Third, the experimentation and implementation of cyber means. Forth to make reassessments and seek further improvements.

Tabarsky (2016) even considers immaterial elements in his analysis. Still, the innovation aspect he puts forward is linked to the economic-military issue, not ideational, encompassing more a situational awareness framework that will lead to action than cyber power formation. In contrast to Tabansky’s case study proposal, thus seeking a more holistic theory, it is worth diving into McCarthy's (2012) proposal.

McCarthy (2012) understands that cyberspace is a domain simultaneously as a global common. He compares strategist authors from the maritime (i.e., Mahan, Corbett) and aerial domains (i.e., Douhet, Mitchell, and Seversky) to find commonalities between them and verify if the military theory can serve as a basis for application in cyberspace. In this sense, he assumes that state interests in cyberspace would be the same in other domains of war. In the word of the author:

> Current international relations theory addressing these domains emphasizes the power relations between international actors and provides a means of assessing their respective abilities to pursue national security interests through, and from, the subject domain. In each of these connective domains, the basic interests of states and other actors is to ensure safe passage for both themselves and their allies while maintaining the ability to deny the same freedoms to their enemies. It is reasonable to assume that state interests in the cyber domain will remain the same as in the more mature domains (MCCARTHY, 2012, p. 59).

McCarthy (2012) validates his hypothesis that military theory can explain cyber power in developing his thesis. He indicates that the foundation of cyber strategic policy and development must be made through military, civil, and commercial uses of the domain, balancing military and economic variables, and investing in developing and creating specific institutions for cyberspace. Faced with these statements, McCarthy turns to theory. He exposed that cyber power theorists must "identify, include, and explain fundamental concepts such as lines of communication; chokepoints; the roles of government, population, and geography; and operational uses, such as direct attack of an enemy's will and means to resist."(MCCARTHY, 2012, p. 289)

In this context, he indicates the importance of discussing a theory of cyber power within four types of operation: control, denial, power projection, and protection. The first means operations that allow your country to use the medium whenever and wherever it wants. The second means operations designed to prevent adversaries from using the medium. The third is operations to project power within the domain to affect adverse cyber operations and affect outside the cyber domain. The last is operations to protect and secure the use of the cyber domain against interference from both within and across domain boundaries (MCCARTHY, 2012, p. 302).

Although well elaborated, McCarthy's proposal (2012) remains focused on material factors of cyberspace (economic, military, geographic, technical), disregarding immaterial elements. These factors could make a difference even in conflictive environments, such as an eventual cyberwar. Furthermore, its proposal rooted in military theory limits the potential use of cyber power to project power in peacetime.

Also, exploring the approximation between cyber power and air power, Anderson (2016) elaborates on a theoretical proposal. This author also deals with cyber power as a domain. He emphasizes that this power would not be limited only to cyberspace but to all instruments of national power (i.e., DIME), as the first theorists did. However, to him, cyber power should not be relegated to just another way of conducting psychological operations. Instead, it should be seen as another tool to shape foreign perceptions of military capabilities (in the case of the United States, which is the author's focus), which would be fundamental for dissuasion.

To Anderson (2016, p.119), as the discussion regarding airpower and its relevance as an independent fighting force in the early 1900s, “so too should cyber power’s unbounded capabilities be explored to determine its role as a military power and its ability to achieve political objectives.” Thus, cyber power could and should have an independent role, but not decisive in itself for the conduct of wars. Therefore, one needs to acknowledge he considers immaterial variables (psychology and deterrence) relevant. Still, his effort is limited in explaining them only in a conflictive context, using the case of Stuxnet as an illustration (ANDERSON, 2016).

In this sense, using Buzan and Little's matrix, the first generation of cyber power theorists tend to stay at the unity analysis level, using especially military and economic analysis sectors. This reflects how realists see cyberspace. In other words, realists see the anarchic international environment prolonged into cyberspace, which, in turn, included in the reasoning of survival for states, leading to the need to have a state-centric vision of cyberspace dynamics. Survival depends on how states correctly assess and use their capabilities. As a continuation of the international realm, it can reflect issues such as the balance of power and is very much attached to the safety and security of critical infrastructures.

In a study on the Balance of Power in Cyberspace, Klimburg and Faesen (2020) acknowledge that the difficulty in knowing what capabilities in cyberspace are, makes it challenging to describe comprehensively what their means are (delivery systems or weapons). But "the common perception of a state's cyber capabilities, even if founded on incomplete knowledge, can function as a basis for calculating the respective balance of power" (KLIMBURG; FAESEN, 2020, p. 149). Another study also concerned with capabilities comes from Demchak (2020). He reflects on the constituency of cyber powers, proposing the term "robust cyber power" to assess states' ability to manifest strategic coherence and appropriate scale in successfully developing national systemic resilience and forward government's disruption capabilities. Focused on the protection of Socio-Technical Economic Systems, Demchak explains that currently, no state is a robust cyber power. However, he alerts that China has demonstrated the most strategic coherence in using its economic and demographic scales to further its security and economic interest (DEMCHAK, 2020).

In this sense, the main disagreement among first-generation theorists is regarding cyber power's status concerning other types of power as an instrument with or without the ability to win wars (CAVELTY, 2018). Furthermore, the main debility of the theories is that they are centered on assessing capabilities, which is hard to do in the digital environment. According to Mary Manjikian (2021, p. 66), given that cyber materials "move quickly across national borders, it may be difficult to know definitely which expertise and which weapons reside within which geographic borders." Moreover, comparing cyber power to other measures of power can be unfruitful. As Manjikian explains, states may have different goals related to their survival, which can result in different requirements for what it means to be cyber-powerful (MANJIKIAN, 2021, p. 78-79). This has not prevented first-generation theorists from influencing further developments in cyber power analysis. However, as other world visions also engaged in the debate, and consequently different International Relations theories as well, other proposals emerged to explain cyber power

2.2.2 The Second Generation of Theorists: A Liberal Basis

Considering conflictive contexts or the need to win and lose wars, the second generation of authors on cyber power will include more explicitly and without so many fears ideational variables, still within a liberal logic. Thus, one of the first examples of this generation is Nye (2011), who identifies that cyber power is different from power based on information resources since one would be new and the other already known in human history. Furthermore, the behavior of cyber power would depend on the set of resources related to “the creation, control, and communication of electronic and computer-based information -- infrastructure, networks, software, human skills” (NYE, 2010, p. 3). In this regard, the cyber power margin would not be restricted to use on the network but would expand to other “extra-cyberspace” domains, corroborating the idea of cyberspace transversality.

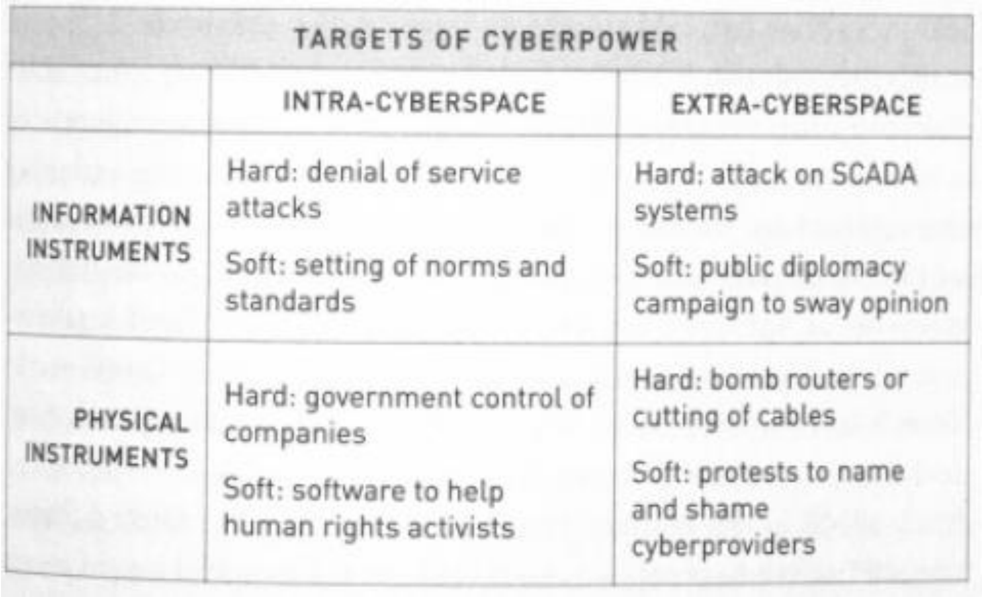
In Nye's logic, the duality of intra and extra cyberspace allows a list of targets for both soft and hard power in cyberspace (Table 6). This way, information instruments can produce soft power in cyberspace through agenda setting, attraction, or persuasion, whereas hard power resources are given in the physical form (NYE, 2011).

Besides, Nye (2011, p.130) analyzes how the three faces of power in the cyber domain could manifest themselves, both in soft and hard forms. The hard power would manifest in the first face by denial of service attacks, malware insertion, ladder system features, and blog arrests. In contrast, the soft power would be manifested via information campaigns to shape hackers' initial preferences. The second face would manifest hard power through firewalls, filters, and pressure on companies to exclude some ideas. In contrast, soft power would manifest itself in self-monitoring Internet Service Providers (ISPs) and search websites, in Internet Corporation for Assigned Names and Numbers (ICANN) rules on accepted software names and domains. Finally, the third face would display hard power via the threat of punishment from bloggers who would disseminate censored material. In contrast, soft power would manifest information in creating preferences, repulse, and norms development.

Thus, Nye (2011) plays with the forms of a multidimensional power in his concept of cyber power, emphasizing the importance of state and non-state actors in a larger context of diffuse power relations in the international scenario. However important, Nye states that although cyber power may create some power shifts among states, it would unlikely be a game changer for power transition. In this regard, he emphasizes that the diffusion of power to non-state actors and network centrality would be a key dimension of power in the 21st century.

Recalling Buzan and Little framework, Nye (2011) focuses his analysis on the capacity for interactions, making it possible for non-state actors to hold cyber power. However, although he puts some structural and institutional notions in his proposal, they are not explored. In addition, intangible elements are confused with material elements in the explanation, making it challenging to track practical capabilities that would identify cyber powers.

Table 6 - Physical and Virtual Dimensions of Cyberpower



TARGETS OF CYBERPOWER		
	INTRA-CYBERSPACE	EXTRA-CYBERSPACE
INFORMATION INSTRUMENTS	Hard: denial of service attacks Soft: setting of norms and standards	Hard: attack on SCADA systems Soft: public diplomacy campaign to sway opinion
PHYSICAL INSTRUMENTS	Hard: government control of companies Soft: software to help human rights activists	Hard: bomb routers or cutting of cables Soft: protests to name and shame cyberproviders

Source: Nye (2011, p. 127).

The idea of non-state actors as holders of cyber power is an element that has begun to gain traction in the second generation of cyber power theorists. Betz and Stevens (2011) are also referenced in this sense. For these authors, power comes within, outside, and through cyberspace as the social relations through which it is staged and constructed, not confined to cyberspace alone. Thus, the authors understand cyber power as the variety of powers circulating in cyberspace. In Betz and Steven (2011, p. 44) words:

> (…) cyber-power can be understood as the variety of powers that circulate in cyberspace and which shape the experiences of those who act in and through cyberspace. (…) Cyber-power ‘is not created simply to exist, but rather to support the attainment of larger objectives ... across the elements of national power – political, diplomatic, informational, military, and economic’.

In this sense, they drew inspiration from Barnett and Duval's sense of multidimensional power and proposed four manifestations of cyber power. The first one is compulsory power, meaning compelling others to do something. The second one is institutional, meaning indirect control through institutional mediation. The third one is structural, meaning how cyber power helps to determine structural positions. The fourth one is productive, meaning the constitution of the social subject through discourse mediated by and enacted in cyberspace (BETZ; STEVENS, 2011).

Concretely, compulsory cyber power translates into control over remote machines and the deployment of non-material resources to affect the actions of others directly. In this sense, Betz and Stevens (2011) comment on how coercive effects would only derive if actors recognized that resources were ordered against them and believed in the credibility of threats against them. Thus, they comment that compulsory power would be tough to implement.

Institutional cyber power translates via the influence of opinions from foreign audiences through media institutions. They give China ns Russia as examples. This is so since these countries use the International Telecommunication Union (ITU) and the Shanghai Cooperation Organization (SCO) to advance their national interests in Global Internet Governance. Furthermore, they explain that institutional power involving non-state actors could ultimately be considered coordinated by the state. Still, it would need to be articulated through a body of intermediaries capable of effecting changes where the liberal state could not (BETZ; STEVENS, 2011).

As for structural cyber power, Betz and Stevens (2011) explain that civil networks, structured around cyberspace tools, opportunities, and forums, could flank and sometimes replace hierarchical industrial sector structures. They illustrate this kind of power in the Arab Spring and the use of social networks to show how positions (i.e., structures) can change through digital pathways. So for the authors, structural cyber power works both to maintain the status quo and disrupt it.

Finally, productive cyber power refers to the issue of discourses in cyberspace. In other words, it serves not only the reproduction and reinforcement of existing discourses in cyberspace but also the construction and dissemination of new discourses (BETZ; STEVENS, 2011). In this sense, one can observe this form of cyber power in the recent phenomenon of Fake News, in terrorist propaganda and counter-propaganda discourses, and in the logic of social networks that create "bubbles" of information that provide feedback to each other. Thus, the authors say, "In an era of ‘strategic communication’ and ‘public diplomacy,’ productive cyber-power is perhaps the most important form of cyber-power” (BETZ; STEVENS, 2011, p. 51).

However, if cyber power is fragmented into several power streams, which would be enough for an international projection? Betz and Stevens do not seem to distinguish in this regard, nor, as characteristic of this second generation of theorists, point to causal links between powers. Equally relevant is that contextual variables also do not seem to weigh the analysis, despite establishing that productive power is the most important in cyber power dynamics.

With a more cohesive theoretical proposal and differentiating itself by considering the elements of cyber power comes the suggestion of Rowland, Rice, and Shenoi (2014). For the authors, cyberspace as a new multidimensional frontier would encompass elements of diplomatic, informational, military, and economic power (i.e., DIME). Both state and non-state actors could achieve cyber power via these instruments. So, in general, “power” would be based on an influential element and the issue of resources consolidated in the aspects of DIME.

From these premises, Rowland, Rice, and Shenoi (2014) develop the vital components of cyber power: ideology, body politic, and infrastructure. In this sense, ideology would bring together cyber entities' values, objectives, and essential behaviors. Moreover, they categorize cyber entity ideologies into three non-disjoint groups based on statehood, legality, and the profit motive.

Statehood would be the responsibility of states towards their citizens. This would be within the idea of creating a contractualist state, where a state is based on the social contract between the state and its citizens to ensure society's well-being is imbued with values and beliefs that legitimize it (i.e., social regime). Thus, Rowland, Rice, and Shenoi (2014) explain that the Cyber State would be very similar to its physical counterpart, exercising its responsibilities via cyberspace but linked to the physical world. In this sense, there would be the possibility of the influence of the Cyber State in the four dimensions of power (DIME). Moreover, since human beings created cyberspace, it reproduces intrinsic realities to humanity as the issue of crime, war, and terrorism. Thus, people would demand Cyber State strategies of their own.

Legality refers to the legislative basis for actions in cyberspace. Here the authors raise questions about borders and jurisdiction since cyberspace threats are transnational, and the physical part of cyberspace (mainly wired media) is under sovereign national territories. The authors explain that “The Internet and the cloud have repeatedly raised questions about the precise locations where criminal activities have occurred and the legal frameworks that apply” (ROWLAND; RICE; SHENOI, 2014, p. 5).

Finally, the profit motive refers to the economic issue of cyberspace. In this sense, the authors explain that a cyber economy would parallel the “real” economy in a relationship of interdependence. However, they warn of two problems within this sphere: the anonymity of individuals and the difficulty of verifying transactions, thus generating the need to build elements that provide trust between buyers and sellers (ROWLAND; RICE; SHENOI, 2014).

The body politic refers to the human component of the cyber state. It would comprise a governmental body and individual members, including shareholders, adherents, and engaged citizens. Thus, according to the authors, there would be a need for a command and control center in cyberspace with various members participating and interacting with the participating members of cyberspace. Furthermore, the authors emphasize that the responsibilities of the body politic would depend on the type of entity, its ideology, and its agenda (ROWLAND; RICE; SHENOI, 2014).

According to the authors, Infrastructure refers to the physical part of cyberspace, comprising human and non-human means, including critical infrastructures. In the author’s words:

> The physical infrastructure of cyber entity encompasses all the physical resources needed for the entity to operate and thrive. At the minimum, this would include hardware, software, data, and networking resources, physical space for operations, and supporting resources such as utilities and fuel. The physical infrastructure also involves components that support the body politic. These include physical living and working space, food and drink, and utilities (ROWLAND; RICE; SHENOI, 2014, p. 6).

The authors also speak on the need for a cyber entity to possess cyberinfrastructure components. The cyber entity must provide a stable, reliable, and secure physical infrastructure to be viable. Something that "entails a notion of sovereignty or the ability to position infrastructure assets in the sovereign domain of another (real-world)entity and operate under the protection of the entity(wittingly or unwittingly)" (ROWLAND; RICE; SHENOI, 2014, p. 6).

The authors further focus on answering what makes up cyber power. Thus, they indicate the need to leverage resources from the five domains of power (air, land, sea, space, and cyberspace) and conduct activities and project influence in four dimensions of power (diplomatic, informational, military, and economic), using four interconnected properties: viability, persistence, resilience, and interdependence, to maintain its attained status (ROWLAND; RICE; SHENOI, 2014).

Viability refers to the fact that cyber power exists and functions. This would be achieved with a body politic, infrastructure, ideology, possession, and power in the four dimensions (DIME). In this sense, the authors emphasize that the informational field can be used in a powerful way to conduct public diplomacy and energize the body politic of the cyber entity. In addition, the military variable becomes relevant but not essential since, just as in the physical world, military power attracts smaller countries to form political alliances. The same can happen in the cyber area (meaning that smaller countries seek protection in cyber in exchange for favors or alliances).

According to the authors, persistence encompasses the ability to design agenda and make the entity's data and software last. In this sense, the first aspect is possible by guaranteeing the functioning of physical and virtual infrastructures. Whereas the second is via the use of the cloud for data storage.

Resilience is "the ability of a system to resist, absorb, recover from, or successfully adapt to a change in environment or conditions" (RICE; ROWLAND; SHENOI, 2014, p. 9). Thus, for the authors, a cyber power would have to have the ability to recover quickly from adversity in cyberspace. For this, its viability components should be individually resilient. In the authors ' opinion, ideology is the "soul" of cyber power.

Finally, Interdependence would be at the heart of cyberspace and the Internet itself. In this sense, the ability to coordinate and command everything in harmony to maintain a good interdependence would generate, in the authors' opinion, the stability of the system as a whole, helping aspects of viability, resilience, and persistence (RICE; ROWLAND; SHENOI, 2014).

It is important to point out that the authors make the reservation that the military variable would be concentrated in the state sphere, suggesting that for them, the total reach of cyber power would only occur via states. In this sense, even if cyber power could be developed with immaterial variables, its totality within the scope of states would only be achieved materially through the military. In addition, when considering ideology as the soul of cyber power in issues related to statehood, economics, and legality, the authors refer us to the idea of a Complex Interdependence, which, although theoretically valid, limits the time to explain conflicting behavior of states.

In summary, although more open to the immaterial variables of cyberspace, which would be reflected in cyber power, the second generation of cyber power theorists still seems not to detail them very well. Even when describing these variables, they do not put them in contextual perspectives. They also tend to analyze the unit level as per the Buzan and Little matrix. The difference with the first generation is the inclusion of non-state actors into the scene.

In this regard, one can think about the power of economic entities. But it is important to highlight that considering the relationships between states and non-state actors, especially companies, they possess different interests since their survival is more attached to consistent profit-making than security itself. Despite owning the majority control of cyberspace infrastructures, no roles are clearly delimited, and inconsistent lines on the definition of cyber power do not favor their case. As Cavelty (2018, p. 7) explains, the second generation of a more liberal/neoliberal nature also relegates cyber power to a secondary space to national power through P/DIME, as an agent that reproduces or subverts existing powers. This could explain the emergence of ideas comparing non-state cyber actors as privateers (EGLOFF, 2022) and mercenaries (MAURER, 2018).

2.2.3 Approaches to the International System

The cyber power theories from the first and second generations gave rise to further studies considering their precepts. Thus, some proposals on understanding cyber power turned to the system level of analysis. Rather than an evolutionary idea, the generational bids start to be developed in parallel, giving space to forming a possible third generation. In this, one can highlight the work of Haaster (2016), Lonergan (2017), Valeriano, Jensen, and Maness (2018), Bebber (2017), Gomez (2013), and Segal (2016).

Haaster (2016) relies on Barnett and Duvall's (2005) idea of power and the cyber power proposals of Betz and Stevens and Nye to build his thinking on cyber power. For him, power analysis must transcend the last century's ideas and understand that power must be analyzed from a relational perspective. Furthermore, Haaster emphasizes that power is dependent on specific policy contingency structures.

In this sense, Haaster (2016) understands that power relations must be perceived through dimensions. These dimensions would be scope, domain, weight, costs, and means, allowing us to determine the receptivity of the actor under the yoke of power. Scope refers to the objective. Domain refers to which actors are involved. Weight refers to the probability of effectiveness. Costs to how costly the action is for A and B compliance. Means to instruments involved (encompassing what several academics put under the DIME/DIMEFIL perspective)[13].

Haaster (2016) then recalls that cyber power tends to be treated as a concept of military doctrine, emphasizing the primary role of information on the battlefield. Besides, he highlights a current division in academics/military around the questioning of cyber operations: whether they would be a subset of information operations or not. However, the author evades this logic and explains that assessing cyber power would involve estimating an actor's ability to transmit power in cyberspace. Thus, his concept of cyber power is based on Betz and Stevens (2011), with a Foucaultian touch. In the author's words:

> (…) cyber power comprises the variety of powers affecting the geographic, physical network, logical, and cyber persona components, which consequently shape the experiences of state and non-state actors who act in and through cyberspace. This includes, for instance, using social-media profiles (the cyber persona component) to affect others; the use of offensive cyber means and methods to digitally compromise a critical system (the logical component); or using law enforcement or military powers to physically establish control over network infrastructure (a physical network component) (HAASTER, 2016, p. 14).

In this way, he parallels Carr and Michael Mann's instruments of power and the logic of authors who use the DIME model on conventional and cyber capabilities. Thus, he realizes that a generalized overview of cyber power distribution cannot exist because it depends on all dimensions of power (contextual and temporal) since there would be many contingencies to be captured in such an overview (HAASTER, 2016).

However, Haaster (2016) states that this does not invalidate power distribution analyses to help decision-makers. The distribution of cyber power, examining the means (e.g., network infrastructure, spending, government cybersecurity budgets, malware acquisition, DDoS capability, IT graduates, etc.) needs to incorporate that results must be interpreted in their context and associated with other dimensions of power.

On the one hand, this position becomes relevant for considering the capacity of previous, realistic, and liberal analyses and the limits or possible frameworks of variables to

[13] According to Haaster (2016, p.18) "There are many other categorisations rivalling or, sometimes, dwarfing the DIMEFIL construct in comprehensiveness and academic stature. This subsection will first briefly discuss the instruments of state power, and then forward an overview of the means enclosed in the DIME, DIMEFIL and other categorisations. After that, these means will be supplemented with cyber capacities described by Nye and Betz & Stevens, and other cyber capacities".

determine a distribution of cyber power at the system level. More pragmatically, the system can lead to distortions, given that different contexts will provide various types of cyber power, and then the questioning by Betz and Steves about which powers would be sufficient for an international projection falls into question.

With a more realistic perspective, we have the analysis of Lonergan (2017). In his thesis, "Cyber Power and the International System," he denies that the cyber domain is predominantly offensive since the specific nature of offensive operations and the destructive potential of a cyber conflict are minimal. The credibility of a threat, translated by capacities and will, is overshadowed by anonymity (secrecy) and the costs between virtual and physical actions and reactions. Thus, cyber warfare strategies would be ineffective if they focused on punishment and risk as forms of intimidation (LONERGAN, 2017).

For Lonergan (2017), as there is no lethality in cyber weapons, states would eventually exhaust their cyber capabilities or find them inert over time as effective defenses are discovered. Even if states tried to combat this trend via resource mobilization, it would take time, defusing any crisis and providing space for governments to decide to slow down, ultimately generating a tit-for-tat game between States (LONERGAN, 2017).

In this sense, cyber power alone would have little power as an instrument of coercion but would not be useless. This is because it could contribute to the credibility of threats, as it would allow a certain verification of the material capabilities of states. This verification could be made through “budgets, growing and training cyber forces, establishing commands, and advertising participation in major cyber exercises” (LONERGAN, 2017, p. 179). Furthermore, the author recognizes that measures of cyber power should include factors beyond crude estimates of the sizes of cyber forces (LONERGAN, 2017, p.180).

Therefore, human resources gain relevance in the digital landscape, which leads us to a more technical and abstract observation of cyber power. In addition, as Lonergan (2017) explains, factors such as the regime type influence. He explains that democratic countries receive a more significant charge concerning monitoring the flow of information by their population than authoritarian countries, requiring more creative alternatives to deal with them with APTs (Advanced Persistent Threats), for example.

Despite Lonergan (2017) mentioning the importance of intangible capabilities to the cyber structure, he understands that at the structure level (i.e., International System), what counts, are economic and military factors. In the author’s words:

> The combination of technical knowhow with financial resources severely limits the number of states that can be called genuine cyber powers—particularly since such investments may be long-term commitments without guaranteed successful outcomes. Indeed, some cyber operations may take years from the time the concept is conceived until the operation is implemented (LONERGAN, 2017, p. 183).

So much of the future of cyber power is tied to government action. In other words, governments may want to use cyber power to pursue war strategies that erode the enemy's ability to resist because of the perceived ease of cost-effectiveness and destruction that conventional asymmetric conditions provide (LONERGAN, 2017, p. 186).

Still, given this scenario, the author states that how states react to cyber-attacks can potentially create spillovers outside the cyber domain. In this sense, they would influence other domains of war, building one survival logic in the face of cyberattacks. For this not to be configured or at least to be mitigated, Lonergan (2017) points to resilience as the most favorable path to strategic advantage, placing the importance of cooperative alliances in this field, such as the Five Eyes Alliance, in the USA case.

Lonergan's (2017) analysis is relevant for conflictive contexts, but focusing on economic and military issues, treating international actors as rational, and setting aside contextual variables makes it challenging to justify behaviors or actions that escape a game of tit-for-tat. These points apply equally to the proposal of Valeriano, Jensen, and Maness that, although not concerned with cyber power but with cyber strategies, analyzes dimensions of state interaction in cyberspace at an international level.

Valeriano, Jensen, and Maness (2018) propose understanding cyber strategies within a context of historical state rivalry, counting on a set of 192 cyber incidents within a period of 14 years (2000-2014) and based on the analysis of the offensive-defensive balance. In this sense, the authors explain that

> Major powers employ cyber strategies to gain a position of advantage relative to their rivals. Small states and nonstate actors attempt to use cyber operations to punch above their weight to maximize their political goals. States have begun to attack their enemies' through cyber operations as well as propaganda spread in comment fields, social media, and cable news broadcasts (VALERIANO; JENSEN; MANESS, 2018, p.1-2).

They further explain that there is a gap in research regarding the understanding of alternatives of measurement to the effects of cyber conflict and its coercive potential. Besides, the “efficacy of power to pressure target position states, shape their behavior, and manage escalation between rivals remains an open question in need of investigation” (VALERIANO; JENSEN; MANESS, 2018, p. 2).

In this regard, the central problem on which the authors are based is the following question: “how do states use cyber strategies to influence their rivals?” (VALERIANO; JENSEN; MANESS, 2018, p. 22) For the authors, the latent capacity of a state as a proxy measure of its cyber power is not a significant predictor of coercive potential. Thus, more traditional arbiters of strategic competition (i.e., economic and military power) would better explain rivalry behaviors (VALERIANO; JENSEN; MANESS, 2018, p. 54).

Seeking to cover the gap, the authors used a “latent cyber capacity” index in their analysis, capturing two forms of cyber power: infrastructure and knowledge capital. The first would include variables related to the countries' connectivity, that is, broadband subscriptions per 1000 people, the number of secure Internet servers per 1 million people, and the percentage of high-tech exports of total manufacturing exports to each country in the period 2000-2014. The second would look at the country's level of education in science, technology, engineering, and mathematics (i.e., STEM) and the personnel who are more likely to manipulate programs or hack. The knowledge capital in this sense included the following variables: the number of Internet users per 1000 people, the absolute number of scientific and technical journal articles published in a country, and the number of residents of each country who applied for patent applications for each year. All variables were collected from World Bank data and mathematically adjusted (z-score) to be positive and normalized for comparison, reaching a score ranging from 02-08 (VALERIANO; JENSEN; MANESS, 2018, p. 59-60).

Thus, what the authors identify were three cyber strategies that states use: cyber disruption (low-cost initiatives that harass the target to influence it to change its decision-making calculation), cyber espionage (efforts focused on changing the balance of information or manipulating digital perceptions to produce beneficial bargaining effects) and cyber degradation (high-cost, high-impact efforts that seek to degrade and destroy critical capabilities through computer networks, destabilizing the enemy) (VALERIANO; JENSEN; MANESS, 2018, p. 225).

The authors found an increasing trend in incidents, but this was due primarily to espionage (52%) and disruption (35%), with degradation actions comprising only 13% of incidents, that is, merely 25 cases of the 192 analyzed. Furthermore, they identified that cyber operations rarely produce concessions with a result of only 5.7% success (VALERIANO; JENSEN; MANESS, 2018, p. 225-6).

Moreover, according to the authors, these strategies are not used in isolation but in a broader context of traditional statesmanship tools to have coercive effectiveness, albeit low. In the authors' words: “New technologies create new challenges but not necessarily new advantages. Cyber degradation works more as a multiplier than a single decisive blow that forces a state to capitulate” (VALERIANO; JENSEN; MANESS, 2018, p. 109).

In addition to these quantitative results, the authors also show that some factors limit cyber strategies:

a) Lack of coercive impact, norms (States do not want to open Pandora's Box);

b) Strategic uncertainty (cyber operations are risky and can represent ambiguous signals); and

c) Spillage (cyber capabilities can be easily copied once released on the Net).

Also, the authors explain that cyber strategies are considered an optimized form of political warfare in the 21st century, which relies on bargaining and ambiguous signaling to help rival countries to gain a relative long-term advantage (VALERIANO; JENSEN; MANESS, 2018, p. 226-227).

Thus, in general, the authors' qualitative-quantitative study reaches the same conclusion as Lonergan (2017) that the power to coercively compel other states in cyberspace is practically nil. In this sense, Valeriano, Jensen, and Maness (2018) speak that efforts should be directed toward creating new norms, sharing information, and stimulating public-private multilateral frameworks to avoid dangerous escalation.

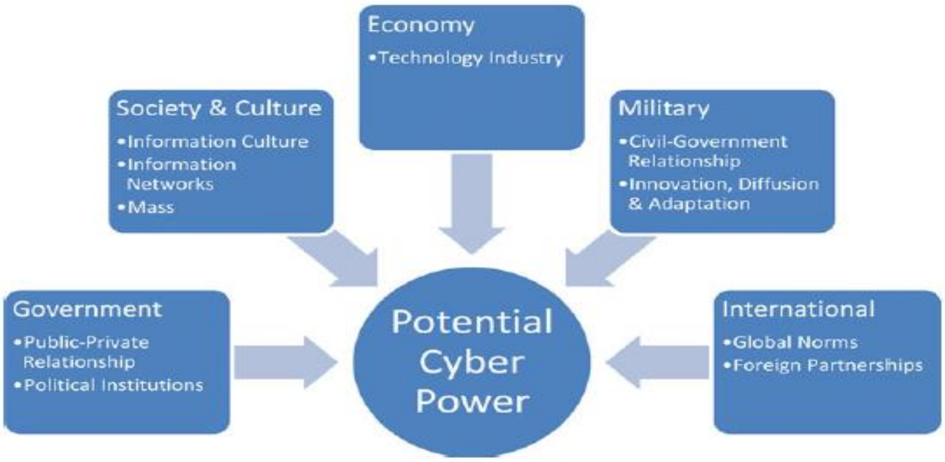
In the same line of potentialities, the proposal of Bebber (2017) follows the path that understands cyber power as the effectiveness of its use. Bebber (2017) works with the concept of potential power, which would be: "the available human and material resources within a strategic environment that can be utilized to generate effects in and through cyberspace. Thus, this type of power would involve domestic (unit level) and systemic variables. While cyber effectiveness would be the "ability to translate cyber power in support of national political ends in and through cyberspace." Besides, an amalgam of resources would be needed to develop potential cyber power (see Figure 4).

Although Bebber (2017) expands the number of variables to be evaluated when talking about cyber power, he emphasizes the coordination and use of this power in the strategic, operational, and tactical scope. In other words, his proposal focuses again on the military sphere by proposing an evaluation of effectiveness based on levels of war within a relational context of competition (between competing States), realizing its limitations of the analysis and leaving for future research hypotheses involving spheres such as the social and economic.

In this sense, the limits of realist approaches to cyber power can be seen again since the ideational variables are shown as relevant but not further developed. Demanding future works with different biases that focus on power relations in the digital realm. One of the first works in this direction appeared in 2013 with the constructivist proposal of Gomez.

Gomez (2013) analyzes the issue of cyber power at the system level since dealing with state interactions. He points out that realism and liberalism are both theoretical lines that fail to provide a uniform explanation for events of cyber conflicts. The problem with realists is that they are based on the assumption that states have equal interests. The problem with liberals is that they believe that state interconnectivity generates vulnerabilities at the same level. In this regard, one of the first cyber power indexes (CPI), prepared by Booze Allen Hamilton, would be out of step in classifying countries and relating it to the number of cyber attacks received by a country. Thus, the author states that from a "constructivist's perspective, the difference may be explained by variations in the attributes that determine a state's cyber power and, consequently, the realities it faces"(GOMEZ, 2013, p. 3).

Figure 4 - The domestic and global factors



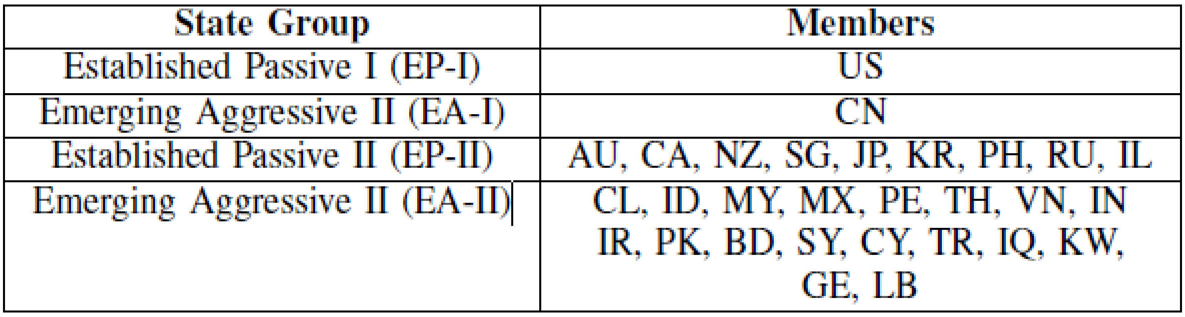
Source: Bebber (2017, p. 427).

Given this finding, the author bases himself on the interdependence of both the offensive capacity and the inherent vulnerability of states to describe the cyber power perceived by them. He mixes the CPI and ideas of Hare (2010), who proposes that a state's military power and socio-political cohesion contribute to identifying vulnerabilities by mapping these factors against the perceived vulnerability of a state. He further assumes that a state's willingness to invest its resources to achieve a specific objective is inversely proportional to its inherent vulnerability that can be exploited by retaliatory action.

Thus, Gomez (2013) identifies 50 individual characteristics he consolidated into six groups: Infrastructure, Economic, Research, Politics and E-Governance, Socio-Political cohesion, and Military Strength. Furthermore, he explains understanding cyber power as reflected in cyber strategies, but only if cyber capabilities are analyzed in the context of past cyber attacks. Thus, it seeks to explore cyber-attacks within 05 parameters: initiator, target, type of attack, attack severity, and frequency, using the database by Valeriano and Maness (2015) and the website Hackmageddon.com.

Gomez (2013, p. 4) thus identifies four groups based on their cyber powers: Established Liabilities I (EP-I); Emerging Aggressive II (EA-I); Established Passive II (EP-II), and Emergent Aggressive II (Table 4). The author explains that states identified as Established Liabilities I and II are seen as the most mature and developed in terms of Infrastructure, Economics, Research, and Policy and Governance existing mechanisms. Since the relationship regarding Cohesion would be more significant in EP-II while with Military Force, it would be more significant in EP-I.

Table 7 - Group Membership



State Group	Members
Established Passive I (EP-I)	US
Emerging Aggressive II (EA-I)	CN
Established Passive II (EP-II)	AU, CA, NZ, SG, JP, KR, PH, RU, IL
Emerging Aggressive II (EA-II)	CL, ID, MY, MX, PE, TH, VN, IN IR, PK, BD, SY, CY, TR, IQ, KW, GE, LB

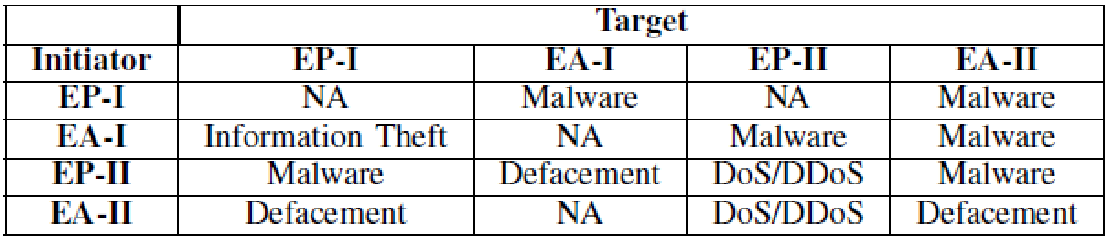
Source: Gomez (© 2013, p. 4).

On the other hand, the groups referring to Emerging Aggressive I and II correlate countries with emerging economies reflecting lower infrastructure, economy, research and politics, and E-Governance. However, showing greater socio-political cohesion and higher military strength compared to EA-I.

Thus, Gomez (2013) realizes that EPI-I and EPI-II countries seek to maintain power at the strategic level, using malware as the main mode of attack against their targets. EA-Is, on the other hand, seek to maneuver their position. That is, their aggressive actions in cyberspace are calculated to minimize the initiator's risk and allow a certain degree of denial through information theft attacks. Finally, the EA-II would "test the waters" since they would be the countries with the least cyber power. That is, they would adopt a strategy to demonstrate the capacity while seeking to minimize the risk of coming into conflict with States that are better off established through more direct DDoS attacks or defacement (See Table 8).

Because of this, Gomez (2013, p. 6) presents three options for strategies that States can adopt in the cyber sphere: maintenance of power, balance maximization, and capacity demonstration. The first could be considered in realist terms, referring to the active use of cyberspace to mitigate perceived threats to state power, hence the importance of military force. The second would refer to the attempt by states to maximize the power they hold to obtain advantages both in cyberspace and in the physical world, but not to the point of triggering a conflict that could jeopardize their current (economic) advantages. As the author puts this second strategy, although it follows realist ideas similar to power maintenance, "it also takes into consideration the implications of being interconnected and the negative consequences this may have on the initiator if this strategy is not utilized judiciously." Finally, the third strategy would serve to avoid escalation or even deescalate existing conflicts since the demonstration of capabilities would give the population the "appearance that a state has responded while less forceful measures, such as negotiations, can take place in the background." (GOMEZ, 2013, p. 6).

Table 8 - Attack Type Matrix



	Target			
Initiator	**EP-I**	**EA-I**	**EP-II**	**EA-II**
EP-I	NA	Malware	NA	Malware
EA-I	Information Theft	NA	Malware	Malware
EP-II	Malware	Defacement	DoS/DDoS	Malware
EA-II	Defacement	NA	DoS/DDoS	Defacement

Source: Gomez (© 2013, p. 5).

It is important to note that Gomez (2013) was one of the few authors explicitly claiming to follow a constructivist path, giving cyber power a more autonomous character. However, he draws many of his insights into realist theory, and by focusing his analysis on cyberattacks, he leaves other fields unexplored. The author acknowledges this, stating that more work is needed to understand this phenomenon, citing as an example the question of how public-private partnerships would follow these guidelines strategies and how they would fit into legality frameworks.

Another author who can also be framed as a constructivist is Segal (2016). He considers the emergence of a new world order, with year zero coming from the Stuxnet worm and the highest point being Snowden's leak of espionage made by the NSA (USA Intelligence Agency). His theoretical framework fits within constructivism because even though he is not concerned with the definition of the cyber power concept itself, he understands that the strongest cyber powers must have the following:

a) Large and technologically advanced economies

b) Public institutions that channel the emergence and private sector innovation,

c) Adventurous and inventive military and intelligence agencies,

d) A compelling story to tell about cyberspace

According to Segal (2016, p.34-38), what matters in determining cyber powers is: The market size (in economic and technological terms). The government's ability to work with the private sector. The behavior of military and intelligence agencies. And the states' narratives in the cyber arena (mainly in Internet governance issues and in legislative proposals at the international level). Thus, for Segal (2016, p.42), the determination of the strategic culture of cyber power use by states would follow five questions about states: “how a nation-state interprets threats, uses force, exerts influence, spurs innovation, and delineates the national good.”

Thus, for Segal (2016), the hacked world order would not be totally chaotic, given that state motivations could be understood through the five guiding questions he posed. Furthermore, “States alternate between political disruption and destruction, platforms and gates, narrative construction and dissembling, mercantilist and innovative intervention, and Hobbesian and Lockean approaches to data and the public good” (SEGAL, 2016, p.49). According to the author, these approaches could be seen as states disrupting, destroying, stealing, commercializing, and influencing.

Finally, it is worth noting that Segal's (2016) view seems to understand cyber power as autonomous and multi-dimensional. Unlike Gomez (2013), the issue of industry and narratives would be developed in the analysis. However, within his logic, Segal (2016, p. 90-92) states that just the United States and China would be the superpowers, and Russia would be on the verge of being one. European states such as the United Kingdom, Germany, and France are relevant, achieving two or three of the necessary characteristics; Israel has potential but follows the US, and Estonia is a vanguard country at the institutional and normative level internationally. Furthermore, he highlights the role of North Korea and Iran as having exceptional international influence and cites Brazil as an important and influential actor in Internet governance issues.

Gomez's (2013) and Segal's (2016) analyses open a range of immaterial/ideational variables in cyber power analysis, especially at the system level. However, a deeper understanding of how these variables are interconnected in moments of stability and instability is still necessary. The quest for comprehending cyber power with the three reasoning lines (realism, liberalism, and constructivism) provided a basis for the three most known cyber power indexes. The next session will explore them.

2.2.4 Cyber Power Indexes

Based on first and second-generation cyber power theories, a group of economists (i.e., economist intelligence unit) sponsored by Booze Allen Hamilton developed the Cyber Power Index (CPI) in 2011. The Index analyzed 19 G20 countries (excluding only the European Union) to measure the success of digital absorption and the quality of the legal and regulatory environment in promoting cybersecurity. For this, the Index was based on qualitative-quantitative research (with UNESCO, World Bacchus, and United Nations Telecommunications Union as quantitative sources) within 04 categories and with 39 sub-indicators, which specifically evaluated attributes of cyber power. Thus, the four categories used by the CPI were: legal and regulatory framework, social and economic context, technological infrastructure, and industrial application.

Indicators within the first category assessed the following elements: government commitment to cyber development (national plan and public-private partnerships); Cyber Protection Policy (Cyber Enforcement Authority, Cyber Security Laws, Cyber Crime Response, International Cyber Security Commitments, and Cyber Security Plan), Cyber Censorship, Policy Effectiveness, and Intellectual Property Protection.

In the second category, indicators evaluated the following elements: educational levels (expected years of schooling and enrollment of tertiary students as a percentage of total enrollments), technical skills (labor productivity growth, research researchers per million people, science and engineering degrees, and literacy in English), trade (ICT exports as a percentage of total exports, ICT imports as total imports and degree of openness to trade) innovative environment (research and development as a percentage of GDP, domestic patent applications, private equity and capital risk as a percentage of GDP).

In the third category, the indicators evaluated the following elements: access to information and communication technology (internet penetration, mobile phones, social media, and Wi-Fi access points per million people), quality of information and communication technologies (fixed broadband per 1000 inhabitants and international internet bandwidth) percentage of GDP spent on communication technology, secure servers, and accessibility of information and communication technology (mobile telephone rates and Internet broadband rates).

Finally, in the last category, the indicators evaluated the following elements: Smart Grids, Electronic Health (i.e., E-Health), Electronic Commerce (within the percentage of Internet users corresponding to requests from companies and individuals and the rate of individuals using Internet Banking), Electronic Government and Intelligent Transport.

Notably, the analysis was based on economic, social, and political elements, subjectively entering the military field by listing critical infrastructures in the industrial application category. Furthermore, the CPI was the first effort ever made at an international level to systematize the distribution of cyber power. In this regard, it would present flaws. Gomez (2013) comments that it does not notice the discrepancy between the classification of locations and the number of cyberattacks suffered by countries. (i.e., not taking into account resilience issues, for example).

About ten years would have passed until new attempts explicitly related to cyber power measurement in an international ranking happened. Amid this period of no indexes productions, or at least no other widely known indexes, the debate was appropriate for constructivists. More research on the other generations showed the need for qualitative and immaterial features to be incorporated. Besides, the theme of cyber power re-emerged within academia due to the technological race between conventional powers and the more frequent and impact cyber attacks the world has seen, including the criminal behavior online amid the COVID-19 pandemic. These efforts resulted in extensive research by the Belfer Center, which launched the 2020 National cyber Power Index (NCPI).

NCPI enlarged the sample of state analysis by measuring 30 countries' cyber capabilities in the context of seven national objectives. It used 32 intent indicators and 27 capability indicators with evidence collected from publicly available data. The index proposed to consider all aspects under the control of a government where possible, presenting what it termed an "all-of-country" approach. Moreover, it considers cyber power "when a country effectively develops cyber capabilities to achieve its national objectives" (VOO *et al.*, 2020, p. 5).

Thus, the research identified seven common objectives that states would want to pursue in cyberspace:

a) Surveilling and Monitoring Domestic Groups;

b) Strengthening and Enhancing National Cyber Defenses;

c) Controlling and Manipulating the Information Environment;

d) Intelligence Gathering and Collection in other Countries for National Security Objectives

e) Growing National Cyber and Technology Competence;

f) Destroying or Disabling an Adversary's Infrastructure and Capabilities;

g) Defining International Cyber Norms and Technical Standards (VOO *et al.*, 2020, p. 21).

Along with the objectives, NCPI collected data on capabilities that they indicate can be categorized under eight themes:

a) Evidence of Attacks;

b) National Online Content;

c) Domestic State Cyber structures;

d) Cyber Vulnerability Mitigation;

e) Private Sector,

f) Trade, and Innovation; Connectivity;

g) Workforce; and

h) Legal and Policy Frameworks (VOO *et al.*, 2020, p. 37).

In this context, NCPI's overall assessment measures the "comprehensiveness" of a country as a cyber actor, observing both material and immaterial features: intent and capabilities. The equation NCPI is demonstrated in Figure 5.

Figure 5 - NCPI Overall Assessment Equation

$$\mathit{National\ Cyber\ Power\ Index\ (NCPI)} = \frac{1}{7}\sum_{x=1}^{7} \mathit{Capability}_x * \mathit{Intent}_x$$

Source: Voo *et al* (2020, p. 2).

NCPI, in this sense, is a significant advance in the debate concerning cyber power. Notwithstanding, it also acknowledges its limitations. These limitations revolve around the lack of publicly available data on cyber capabilities, lack of data on cyber proxies[14], simplifications, and capturing the duality of cyber capabilities[15]. In this sense, NCPI reiterated its understanding that "there is no single measure of cyber power" and that the elements of cyber power should be considered contextually within a state's national objectives (VOO *et al.,* 2020, p. 1). Thus, building on the previous understanding that power is relative.

NCPI, in its format, has embraced the idea developed by the theorists of cyber power that view the phenomenon as multifaceted. However, the contextualization of NCPI still presents itself as limited in understanding why some strategic objectives are preferred over others or even some capabilities. This indeed would need a more in-depth qualitative analysis, which another index, launched in 2021, tried to pursue.

The International Institute for Strategic Studies (IISS) has undertaken a two-year study of the issue launching in June 2021 a qualitative study on cyber capabilities and states' power. The report named "Cyber Capabilities and National Power: A Net Assessment" took a direction similar to Gomez (2013). The report sought to have a holistic approach. Due to its qualitative character, it chose to "apply the methodology to most of the significant current cyber powers and to a small selection of developing powers, before applying it to a broader range of states in due course "(IISS, 2021, p. 4). Therefore it analyzed a total of 15 countries, the majority of the states related to the Five Eyes Alliance (in a position either within, in alignment, or seen as a threat to this group) and the other four (Vietnam, Malaysia, India, and Indonesia) were considered as developing cyber states.

Interestingly the research assessed each country using seven categories:

a) Strategy and doctrine;
b) Governance, command, and control;
c) Core cyber-intelligence capability;
d) Cyber empowerment and dependence;
e) Cyber security and resilience;
f) Global leadership in cyberspace affairs;
g) Offensive cyber capability

In this regard, the research analyzed government documents under the first category, while the second encompassed top-level and operational government and military structures. The third

[14] NCPI have not included the power of cyber mercenaries affiliated or not with government. I also included as proxy the power held by some non-state actors (ex. technology companies) and cyber operations (ex, the existence of cyber military strategies and attribution of state-sponsored attacks) (VOO *et al.,* 2020, p.17).

[15] The research indicated that "some capabilities add to cyber power in one national objective but are detrimental or another" and that "certain data can be both a measure of intent and capability" (VOO *et al*, 2020, p. 19).

category was explained to be hard to measure, given the lack of publicly available information objectively, and so many sources of information were used. The fourth category focused on the vibrancy and scale of the country's digital economy, including its international relationships[16]. The fifth category involved the state's cybersecurity capabilities, including its ability to respond to, and recover from, significant cyber incidents and emergencies, plus the setting of security standards, technical innovation, sector-specific risk management, the effectiveness of the indigenous cybersecurity industry, and the degree to which the country has been able to develop and expand a cyber specialist workforce. The sixth category included relevant international diplomacy, formal alliances, engagement in international forums, international technical cooperation, and arrangements for mutual assistance. The final category involved cyber operations ranging from those designed for cognitive effects to those designed for physical destruction (IISS, 2021).

Differently from the NCPI, the IISS qualitative report explained that "The amount of publicly available data on cyber capabilities is greater than might be expected, making feasible some objective measurement" (IISS, 2021, p. 4). This can give us a hint on how to take a more qualitative look at the issue, leading to more insights into its explanation. Besides, the methodology employed also used insights from interviews with experts. Interviews, in this sense, can shed light on more invisible aspects of the phenomena, making a tool worth further exploring.

Instead of ranking countries, the IISS Net Assessment divided them into three tiers: world-leading strengths in all the categories in the methodology (Tier 1), world-leading strengths in some of the categories (Tier 2), strengths or potential strengths in some of the categories but significant weaknesses in others (Tier 3). In its analysis, only USA was placed in Tier 1. Seven countries remained in the other Tiers: Australia, Canada, China, France, Israel, Russia, and the United Kingdom, placed in Tier 2. While India, Indonesia, Iran, Japan, Malaysia, North Korea, and Vietnam are in Tier 3 (IISS, 2021).

The overall analysis presented by the IISS Net Assessment revealed some interesting insights, such as "*core cyber-intelligence capability* is the primary foundation of cyber power" (i.e., providing situational awareness) (IISS, 2021, p. 171). Another two exciting insights were that most cyber-capable states prefer to see and maintain cyberspace and that the multistakeholder environment (since they pursue a whole-of-a-society approach) and the balance of information are superseding the idea of a balance of power.

[16] It is pointed that the used assessments of research into and use of artificial intelligence (AI) as a proxy indicator for scientific and technological foundation of each country (IISS, 2021, p. 3).

Still, other insights make clear that nuances in states' cyber reasoning and perceptions are needed. This is true especially when the report points out variations regarding the balance between cybersecurity and intelligence policies and the political and military uses of cyber assets. In this regard, national differences play a role in governance, command, and control arrangements. The same goes for tensions between the ICT’s global character and national ambitions for domestic industrial developments (IISS, 2021).

Comparing all three indexes proposals, one can realize they each present flaws. Notwithstanding, they present similarities worth highlighting in the broader debate over cyber power. The first typical trace is the selection of certain countries. All three indexes analyzed Australia, Canada, France, Japan, the United Kingdom, and the United States. This can lead to an overall perception of the relevance of these actors in the cyber realm. At the same time, it can signalize the dismissal of other countries that could bring different aspects to the phenomena analysis.

The second interesting point is that the United Kingdom, the United States, France, and Japan do not vary greatly in classification. In CPI, the UK ranked 1st place, in NCPI the 2nd place, and in the Net Assessment, it stayed within Tier 2 (an intermediary level). Almost the same happened with the USA since CPI ranked 2nd place, NCPI 1st place, and Net Assessment in Tier 1 (top-level). Regarding France, it remained in the same position in CPI and NCPI (6th position) and was placed in Tier 2 in the Net Assessment. While Japan ranked 8th in CPI, 9th in NCPI, and placement in the Net Assessment in Tier 3(low-level). In this context, especially regarding France and Japan, this can either lead to assumptions of either minor cyber capabilities improvements (over at least ten years) or the lack of analysis tools to grasp the advances made in these countries.

In this sense, the following section proposes a different starting point to understand cyber power, seeking to grasp the missing nuances needed to develop the debate further and contribute to the building blocks of knowledge that the constructivist and qualitative studies have been presenting to the overall research of the topic.

2.2.5 Knowledge Building Block: A Constructivist Approach

The literature review shows that cyber power is not straightforward. Cyberspace merges material and immaterial elements that have not been openly documented. Notwithstanding, the new constructivist turn in studies and analysis n provides larger maneuver room for interpretations and paths to assess and understand cyber power.

In this regard, the present thesis aims to take previous efforts that possess a mind-world dualism ontology. Cyberspace is a human creation, and its agents construct such. More specifically, if one considers the physical component of cyberspace, which functions autonomously, the digital environment *per se* is co-constituted by its structure and agency. Thus, a constructivist approach to it seems adequate.

Moreover, as both the first and second generations of cyber power theorists acknowledge, states intend to use cyberspace strategically. Therefore, mirroring some dynamics of the International System. In this regard and considering a constructivist approach, recall Alexander Wendt seems an excellent fit to analyze power dynamics in the digital realm. In this sense, cyberspace can be understood as "what states make of it." If so, the role of the agency needs to be further developed.

Not only states are relevant in cyberspace. Ideas of power diffusion and the relevance of non-state actors, as either mercenaries or privateers, make this point clear. However, taking into account that most states perceive cyberspace as an anarchic structure because they replicate their understanding of the International System to the digital environment. Because they are seen by default as responsible for society's security, their understanding of cyber is worth considering in shaping the digital realm.

So, suppose states deserve attention, but they deal with an environment along with other cyber actors, establishing governance relationships while clearly maintaining asymmetric relationships. In that case, one can infer that cyberspace needs not only to be considered a place of risks, such as the risk of cyber conflict escalation, but also an uncertain place. The uncertainty of cyberspace comes from the lack of complete situational awareness. Big data play a significant role in this sense, and states seeking it through intelligence, as the Net Assessment research demonstrated, is good evidence of the uncertainty element. Thus, one can recall the idea of protean power explained by Katzenstein and Seybert (2018).

Protean power manifests itself in an uncertain environment and is attached to innovation. Despite innovation in the cyber realm not being new, as the literature review showed, considering it taking into account creativity and agility is another entirely different approach. Furthermore, cyberspace comprises loose networks and can be viewed as an open system. Thus, the idea of "power to" and "power with" intertwined can provide new insights and perhaps establish the broader causality links that cyber power research lacks in the present moment.

In short, taking the idea of control and protean power, plus acknowledging that cyberspace is what states make of it, the present research seeks to shed light on states' perceptions of cyber power, which can be translated into key elements. In a way, the study does the inverse role of other efforts since it departs from perceptions to the actual capabilities that matter. It also set a more controlled sample at the subsystem level (as in Buzan and Little matrix). This is so because the focus is on Europe, with three study cases United Kingdom, France, and Germany.

Moreover, using the qualitative analysis coupled with interviews, the research does not aim to group and list the relevant strategic topics for states, such as NCPI and Net assessment. Instead, it seeks to display how these countries perceive power in cyberspace more broadly—further developing what threats are seen and the perceptions that construct their "cyber mentality." The findings of these questions will not be absolute but can contribute significantly to the building blocks of knowledge and understanding of cyber power.

2.3 PARTIAL CONCLUSIONS

The present chapter aimed to do a literature review on cyber power theories, initially explaining how understandings from Political Science and ontologies from International Relations are linked and influenced the theories and concepts set so far on cyber power. In this, it builds upon the emergence of a more constructivist approach toward the issue, incorporating qualitative studies insights to propose a different look toward the phenomenon of cyber power. This approach is a mix of the idea of control and protean power displayed by Katzenstein and Sybert (2018) with ideas from the International System functioning derived by Alexander Wendt (1999, 1992), in which it is understood that cyberspace is what states make of it. In this regard, it departs from the element of agency, not the structure itself, focusing on how perception shapes digital reality. Thus, the following chapters will start the analysis proposed in this thesis by taking an in-depth look into the individual selected countries in search of perceptions over cyber power and their digital mentalities.

3 THE UNITED KINGDOM: DIGITAL MENTALITY AND CYBER POWER PERCEPTION

The present chapter presents the United Kingdom's digital mentality evolution through time and the state's perception of power and cyberspace along this evolution. In this sense, "digital mentality" is being understood here as the state's self-perception linked to its threat perception. Thus, the chapter is divided into three subsections: general context and the phases of the UK's digital mentality, interviews inputs on cyber power perceptions, and partial conclusions.

3.1 THE UK'S DIGITAL MENTALITY

One can track the United Kingdom's concern over the digital world's perils back to the 1990s, with the creation of the Computer Misuse Act (CMA)[17]. This Act was created as a response to the hacking of the username and password of an IT engineer (who worked for a large telephone communications company) that enabled two hackers to access the mailbox of Prince Philip and could not be prosecuted under the current legislative framework (NCA, 2022). In this regard, the Act was elaborated to set out the offenses related to computer interference and the associated tools which enabled computer systems to be breached (HOME OFFICE, 2015), making it the first attempt to deal with the unauthorized access and modification of data. The UK government would face more hacking episodes, including some involving international state actors.

In this context, the Communications-Electronics Security Group (CESG)[18] recognized in 2001 for the first time the importance of protecting data security, recommending the appointment of a central sponsor to determine policy on managing and securing government data (NAO, 2013). Two years later, the UK launched the Information Assurance (IA) Strategy, which addressed the first steps for the UK in assuring the confidentiality of information and communications technology systems and the information they handle. The Strategy was later updated in 2007, broadening the scope of information security to include availability, integrity, non-repudiation, and authentication and encompassing the Transformational Government Agenda.[19] (NAO, 2013; CABINET OFFICE, 2007). The 2007 IA Strategy set a vision for

[17] The CMA was amended in 2015, generating the Serious Crime Act.

[18] An agency within the Government Communications Headquarters (GCHQ).

[19] According to John Hutton's speech (2005), the "Strategy for Transformational Government: enabled by technology" described the "opportunity provided by technology to transform business of Government and how

2011: “A UK environment where citizens, business and government use and enjoy the full benefits of information systems with confidence" (CABINET OFFICE, 2007, p. 4). Moreover, it highlighted as threats the "malicious activity aimed at disrupting information and/or information systems," reflected in the rise of e-crime and ID fraud, and the "compromise by organizational 'insiders'" (malicious or nor). The IA Strategy also posed that "compromise can result in the disruption or even breakdown of services and significant financial and computational losses" and that the scale of the threats was drawn from the Department of Trade and Industry Security Survey (CABINET OFFICE, 2007, p. 5).

Despite the UK government's efforts to secure information and the digital space, two severe data losses, in Her Majesty Revenue & Customs (2007) and the Ministry of Defense (2008), negatively impacted the government's reputation. This was so because these incidents' reviews revealed that information security was not a management priority (NAO, 2013). These episodes and others listed in the Significant Cyber Incidents list of the Center for Strategic & International Studies (CSIS, 2022)[20] demonstrated that the UK government was not protected as it intended. It also highlighted state actors (namely Russia and China) penetrating relevant government systems.

Following a reactive direction, the UK government launched 2008 its first National Security Strategy (NSS), in which the threat of cyber attacks was mentioned. The 2008 NSS had 64 pages and cited "cyber" 7 times, "Internet" 8 times, and technology 11 times. The text listed terrorist, criminal, and state-led cyberattacks as threats. Technology was the second set of challenges and vulnerabilities (behind the economic one) (CABINET OFFICE, 2008, p. 20). In this regard, the NSS said, "it becomes even more important to manage the risk of disruption to their [electronic information and communication systems] integrity and availability through cyber-attack." Besides, it stressed that the Internet was "both a target and opportunity for hostile states, terrorists and criminals" (CABINET OFFICE, 2008, p. 21).

Still, in 2008, the UK government commissioned an independent reviewer to report on how well the government was protecting and managing information. The report, known as the "Coleman Report: Protecting government information," raised an adverse scenario. The report pointed out that the UK lacked a cohesive approach to cyber among the government departments. It said: "Exceptions to central policy are often allowed making it difficult to have confidence in government Information Assurance, and some shared service

that opportunity might be seized," focusing on the transformation of public services, "the efficiency of corporate services and infrastructure of Government organizations," and the necessary steps "to achieve a more professional and effective delivery of technology-enabled business change within Government".

[20] The CSIS list shows six episodes of cyber incidents involving the UK (BETWEEN 2006; 2008).

environments are now not trusted by users, resulting in extra expenditure" (COLEMAN, 2008, p. 23). Moreover, it highlighted there was no role in place to “provide Independent Oversight that the appropriate Governance; Information Risk Management; Policy and Operations; and Monitoring and Controls around Information Assurance are in place across departments and agencies” (COLEMAN, 2008, p. 19) and that “Risk assessment is patchy leaving many without a clear understanding of the risks they are facing or exposing their stakeholders to” (COLEMAN, 2008, p. 20).

Considering the listing of terrorism as a threat amid the digital realm and Coleman's Report, interestingly, the Parliament’s Intelligence and Security Committee (ISC), in its annual report (2007-2008), indicated movements of the GCHQ toward "the potential cyber-terrorist threat (ISC, 2009, p. 12). The Committee's report also highlighted that updates of CONTEST[21]and PREVENT[22] showed that a better understanding of “what led individuals from different communities, including […] cyberspace, to develop extremist views and support or engage in violent extremist” (ISC, 2009, p. 37).

Amid this context, the UK government launched in June 2009 its first National Cyber Security Strategy, which can be considered the country's first step toward its digital mentality development.

3.1.1 The first phase (2009-2015): Market-Driven approach

The "Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyberspace" indicates already in the title the UK's vision for cyber security, meaning to have a safe, secure and resilient cyberspace. Nevertheless, understanding that first is essential to observe what the UK considers cyberspace. Thus, according to the 2009 NCSS, cyberspace "encompasses all forms of networked, digital activities; this includes the content of, and actions conducted through digital networks" (CABINET OFFICE, 2009a, p. 7). At the same time, cyber security would embrace “both the protection of UK interest in cyber space and also the pursuit of wider UK security policy through exploitation of the many opportunities that cyberspace offers” (CABINET OFFICE, 2009a, p. 9). This idea of cyber security is

[21]CONTEST is the acronym for Counter-Terrorism Strategy. The aim of the Strategy is "to reduce the risk to the UK and its interests overseas from terrorism so that people can go about their lives freely and with confidence" (UK GOV, 2011, para 1).

[22]PREVENT is one part of the UK's CONTEST Counter-Terrorism Strategy. It is "unique in that it involves all parts of Government, such as the Home Office, the Cabinet Office, the Foreign and Commonwealth Office, and the Department for International Development" (ESRC, 2022, p. 1). Moreover, it addresses three distinct themes: challenging the ideology that supports terrorism and those who promote it, protecting vulnerable people, and supporting sectors and institutions where there are risks of radicalization (ESRC, 2022, p. 2)

broader than the one related to Information Assurance (IA). IA for the UK would be directed to the "best management of the full spectrum of information security risks, including people, processes, technology, and information assets." At the same time, cybersecurity would include elements "classified, as part of a coherent strategic approach to all aspects of security of data and cyberspace, as well as the exploitation of opportunities to enhance the UK's overall security" (CABINET OFFICE, 2009a, p. 24).

The concepts displayed are built on the UK's idea of taking advantage of the digital economy. The NCSS states, "Developments in cyber space are gathering pace so is the degree to which we utilize them. This offers opportunities for our economy and hence our prosperity" (CABINET OFFICE, 2009a, p. 8). Moreover, the tone of the Strategy becomes clearly market-driven when one observes that the Strategy highlights that cybersecurity should not “discourage the use of new technologies” (CABINET OFFICE, 2009a, p. 9). In this sense, the market-driven approach of the 2009 NCSS recalls the Government's Digital Britain Strategy, which aimed to make the UK the "leading major economy for innovation, investment, and quality in the digital and communications industries" (CABINET OFFICE, 2009a, p. 9). Interestingly, the Digital Britain Strategy (2009) fostered knowledge transfer networks, including a Cyber Security one (TECHNOLOGY STRATEGY BOARD, 2009, p. 13). Thus, one can infer that considering the UK's cyber scenario and the influence of the findings from Coleman's report, the idea of intertwining cyber security with the digital economy appeared to be an obvious path for the country. Indeed, if one looks at traditional power elements translated to the NCSS, the economy took the lead in the UK’s reasoning.

The objectives of the 2009 NCSS encompassed reducing the risk and exploiting opportunities in cyberspace, and improving knowledge, capabilities, and decision-making. To achieve these objectives, the UK would, among other points, "reduce the threat of cyber operations by reducing an adversary's motivation and capability," "gather intelligence on threat actors," "intervene against adversaries," develop doctrine and policy and governance and decision making" (CABINET OFFICE, 2009a, p. 16). The first cited action could be interpreted as a deterrence approach. However, this word has not appeared in this document. Developing doctrine, policy, governance, and decision-making could be interpreted as an effort for coherence (a gap previously highlighted). However, the employment of intelligence is more interesting, which points to another element of conventional power displayed in the UK's reasoning: information.

The 2009 Strategy wisely highlighted some principles, possibly to counterbalance the impact of stating that both capabilities would be developed and intelligence would be employed. These principles included the usual tenets of democratic nations, such as human rights, the rule of law, justice, legitimate and accountable government, freedom, tolerance, and opportunity for all. However, what calls attention is the emphasis on ethics. The Strategy states:

> Cyber security poses particular challenges in meeting tests of necessity and proportionality, as the distributed, de-centralised form of cyberspace means that a wide range of tools must be deployed to tackle those who wish to use it to harm the UK's interests. A clear foundation and appropriate safeguards on use are essential to ensure that the power of these tools is not abused (CABINET OFFICE, 2009a, p. 10).

In this regard, a vision of "power to control" is embedded in the Strategy. Along with some ideas of "protean power." This last linked to the innovation perspective derived from the possibilities of the digital economy and economic influence in the international arena. Still, at this moment, the concept of power appears detached from cyberspace itself as it is directed toward "the tools" employed in it.

Besides the economic and informational elements of conventional power transposed to the digital realm, one can also point to the military, even though it appeared subtly in the 2009 NCSS. The NCSS indicated that “Cyber space is linked to almost all of the security challenges in the *National Security Strategy”* and thus pointed concretely that evolving threats included criminals, terrorists, and states. However, what calls attention is that the reasons for malicious cyber activity are listed as "espionage, influence or even warfare” (CABINET OFFICE, 2009a, p. 12).

The mention of warfare in the Strategy is further explained subjectively. According to the Strategy, "There is an ongoing and broad debate regarding what 'cyber war' might entail, but it is a point of consensus that with growing dependence upon cyberspace, the defence and exploitation of information systems are increasingly important issues" (CABINET OFFICE, 2009a, p.14). In this regard, the international repercussion of cyber attacks in Estonia (2007)[23]and Georgia (2008)[24]might have contributed to the warfare mentioned in the Strategy.

Regardless of the impact of these external events, with the NCSS 2009, an update of the NSS was also launched. The document was titled "The National Security Strategy of the

[23]“Estonian government networks were harassed by denial of service attack by unknown foreign intruders, most likely at the behest of Russian government. Some government online services were temporarily disrupted, and online baking was halted." (CSIS, 2022, p. 67).

[24]“Computer networks in Georgia were hacked by unknown foreign intruders, most likely at the behest of the Russian government. Much press attention was given to annoying graffiti on Georgian government websites. There was little or no disruption of services, but the hacks did put political pressure on the Georgian government and were coordinated with Russian military actions” (CSIS, 2022, p. 65).

United Kingdom: Update 2009 Security for the Next Generation", and the word “cyber” appeared 85 times, the word "Internet" appeared 12 times, and the word "digital" 10 times.

Moreover, the 2009 NSS reiterates that technology is a security challenge (CABINET OFFICE, 2009b, p. 40). Cybersecurity is an important security domain (CABINET OFFICE, 2009b, p. 43), and "some states may look to develop cyber attack capabilities” (CABINET OFFICE, 2009b, p. 41). Still, the government ranked cyberattacks below climate change, terrorism, failed states, and the banking crisis as key risks to UK national security (NAO, 2013, p. 10). Interestingly, the 2009 NCSS clarified that cyber-attacks are treated as below the threshold of war. The 2009 NSS states that:

> Instead of taking offensive military action, there is a realistic possibility […] that a state may seek to threaten the stability or freedom of action of the UK, its overseas territories, or its allies through non-military means by, for example: […] To achieve these effects a state may choose to employ a number of different levers such as cyber attack or espionage (both human and technical) or bring to bear significant economic trade pressure (CABINET OFFICE, 2009b, p. 65).

In this context, the Foreword of the Minister in the 2009 NSS clearly explains the country's digital mentality at that point:

> Our approach means we are responsive to new challenges like cyber security. Seizing the benefits of new technology is vital for our national prosperity. But hostile states, terrorists, and criminals can all potentially use cyber space to undermine our interests. This could be at the national level – for example, through attacks on our essential infrastructure. But security threats in cyber space also threaten the interests of businesses and individuals […] So today, alongside this strategy update, we are publishing the United Kingdom's first national strategy for cyber security to help people make the most of the benefits of Digital Britain in a safe and secure way (CABINET OFFICE, 2009b, p 3-4).

Again, the economic element indicates a desire and self-perception as an emerging “digital economy power,” The "other" materialized in three categories: states, terrorists, and criminals.

Besides these elements of conventional power, more pragmatically, the 2009 Cyber Strategy also indicated institutional creations: the Cyber Security Operations Center (CSOC) and the Office of Cyber Security (OCS). The CSOC was conceived as a multi-agency hosted by the GCHQ to "monitor developments in cyber space (ultimately promoting situational awareness), analyse trends, and to improve technical response coordination to cyber incidents"(CABINET OFFICE, 2009a, p. 17). While the OCS was conceived as a centering strategic element, providing coherence (pointed out in Coleman's Report) and having "overall ownership" of the NCSS (CABINET OFFICE, 2009a, p. 17). Moreover, it would be acting accordingly to a program organized in 8 workstreams:

a) Safe, Secure, and Resilient Systems;
b) Policy, doctrine, Legal and regulatory issues;
c) Awareness and Culture Change;
d) Skills and Education;
e) Technical Capabilities & Research and developments;
f) Exploitation;
g) International Engagement;
h) Governance, Roles, and Responsibilities.

Thus, it was designed to provide "strategic leadership across government for cyber security issues" and placed within the Cabinet Office (CABINET OFFICE, 2009a, p. 17).

Interestingly, despite the involvement of an intelligence agency within the cyber security context, the Intelligence and Security Committee Annual Report 2008-2009 stated the establishment of the two agencies was a "notable development."However, the Committee manifested its disappointment for not having been given "sufficient notification to have been able to include any further assessment of the strategy in this report" (ISC, 2010, p. 10).

Along with establishing the agencies, 2010 was an important year for international cyber policy. The Stuxnet malware triggered the debate on states developing cyber weapons and the possibility of a cyber attack interfering with critical infrastructure. The malware Stuxnet was even cited in UK’s 2010 NSS, but it emphasized that "Although no damage to the UK has been done as a result [of Stuxnet], it is an example of the realities of the dangers of our interconnected world" (HMG, 2010a, p. 30). In this sense, “hostile attacks upon UK cyber space by other states and large scale cyber crime" was placed in the Tier One of the national priority risks (HMG, 2010a, p. 27). The 2010 NSS also reinforced the idea of cyber threats coming from terrorists, criminals, and states, and according to it:

> Activity in cyberspace will continue to evolve as a direct national security and economic threat, as it is refined as a means of espionage and crime, and continues to grow as a terrorist enabler, as well as military weapons for use by states and possibly others. But **getting our cyber security priorities right across the full spectrum of activities is also a great opportunity for the UK** to capitalise on our national economic security **comparative advantages (**HMG, 2010a, p. 29).

Complementary to the new NSS, the UK government published its first Strategic Defence and Security Review (SDSR) titled "Securing Britain in an Age of Uncertainty." The SDRS announced the creation of a "National Cybersecurity Programme" to "close the gap between the requirements of a modern digital economy and the rapidly growing risks associated with cyber space" (HMG, 2010b, p. 47) and which would be supported by £ 650 million over four years (2011 to 2015). Also, the UK, indicating that "future conflicts would use cyber operations in parallel with more conventional actions in the maritime, land and air environments," decided to transform its "cyber capabilities within Defence" by creating a Cyber Operations Group within the Ministry of Defense (MoD). This group would support UK's and its allies' cyber operations to secure "vital networks" (e.g., critical infrastructure) and guide the development of new cyber capabilities. Moreover, the group was tasked to work "closely with other government departments and industry and help forge strong international alliances to increase resilience and joint operational capabilities"(HMG, 2010b, p. 27).

In addition to the previous developments, the SDRS also indicated the establishment of a "new Infrastructure Security and Resilience Council" to improve public-private relations related to national infrastructure, to improve the resilience "to all kinds of hazards and threats, particularly with regard to cyber attacks" (HMG, 2010b, p. 49). This movement reinforces the private sector's engagement, which the UK was pushing forward initially, and the country's view of a holistic engagement of cyber actors, mentioned in the first NCSS. However, the most interesting mentions in SDRS would involve intelligence and alliances.

The 2010 SDRS indicated that intelligence agencies would provide a "sufficient technical platform for the cyber security programme" to keep pace with technological developments and envisioning demands from the Olympics in 2012. The document also highlighted that intelligence capabilities would identify "threats and opportunities early" (HMG, 2010b, p. 43).

Concerning alliances, the 2010 SDRS indicated a political will for more profound proximity with the USA (HMG, 2010b, p.48). Also, at the multilateral level, within the United Nations (UN), to "ensure that governance of cyber space develops appropriate," and with North Atlantic Treaty Organization (NATO), recognizing the organization's wider role in responding to new threats such as cyber attacks, "including by supporting the renewed emphasis on consultation under Article V of the Washington Treaty" (HMG, 2010b, p. 62). These movements demonstrate the further scaling of the UK's international "agenda-setting" mindset and its views on cyberspace as a conflict domain. Regarding this last point, one must remember that Article V of the Washing Treaty refers to collective defense (meaning that an attack against one Ally is considered an attack against all Allies). Besides, its discussion of applications for cyber attacks was raised during the cyber attacks on Estonia in 2007.

Motivated by these debates, the UK government launched, in 2011, a new Cyber Security Strategy titled: "The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world."The new Cyber Strategy was designed to set the UK's cybersecurity vision until 2015. This vision was "to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society" (CABINET OFFICE, 2011, p. 21).

To achieve this vision, the 2011 NCSS set four main objectives:

a) To tackle cyber crime and be one of the most secure places in the world to do business in cyberspace.

b) To be more resilient to cyber-attacks and better protect the UK’s interest in cyberspace.

c) To have helped shape an open, stable, and vibrant cyberspace that the UK public can use safely and supports societies.

d) To have the cross-cutting knowledge, skills, and capability, it needs to underpin all our cyber security objectives.

Among these objectives, the third one calls attention since it presents a more proactive posture from the UK toward cyberspace. It follows the 2010 NSS's idea of responding to security challenges by "ensuring a secure and resilient UK" and "shaping a stable world" (HMG, 2010a, p.22). One can infer that a diplomatic element of conventional power was aggregated into the country's digital mentality.

The diplomatic element would be critical in the four-year time frame of the NCSS. It triggered what has been known as the London Process: a series of multistakeholder meetings held biennially under the name Global Conference on Cyberspace (GCCS) (VAN HORENBEECK, 2018). These meetings focused on implementing principles for governing behavior in cyberspace. They set an agenda for future work building on the existing World Summit on Information Society (WSIS) process (FCO; HAGUE, 2011; VAN HORENBEECK, 2018). The UK chaired the first inspirational meeting of the process, initially titled The London Conference on Cyberspace, which focused the discussion on five topics: economic growth and development, social benefits, safe and reliable access, international security, and cybercrime (FCO; HAGUE, 2011).

Besides this diplomatic element, the 2011 NCSS reinforced the UK perceived cyber threats. These threats followed the previous categorization of criminals, states, and terrorists, but this time politically-motivated activist groups (hacktivists) appeared stressed as well. In this sense, hacktivists were pointed as targeting (with cyberattacks) public and private sector websites to disrupt, cause reputational and financial damage, and gain publicity. Nonetheless, what calls attention is that the Strategy highlights that with cyberspace being borderless and the Internet anonymous in nature, "precise attribution is often difficult, and the distinction between adversaries is increased blurred" (CABINET OFFICE, 2011, p.16). This reminds the emphasis on intelligence capability.

The 2010-2011 Intelligence and Security Committee Annual Report highlighted that was concern about the "GCHQ's inability to retain a suitable cadre of internet specialists," suggesting to investigate of what could be done "within existing pay constraints to improve the situation" (ISC, 2011, p. 20). Besides this recommendation, the 2010-2011 ISC report took a deeper look into cyber, emphasizing that "The intelligence and security Agencies have a key role to play in tackling the cyber threat to the UK." Moreover, GCHQ's work toward cybersecurity would act in four categories: protection, analysis, intelligence-gathering, and military capability (ISC, 2011, p. 58).

In alignment with the ISC report, the 2011 NCSS stated, "The intelligence agencies and Ministry of Defence have a strong role in improving our understanding of – and reducing- the vulnerabilities and threats the UK faces in cyberspace" (CABINET OFFICE, 2011, p. 25). Besides, it displayed a graphic showing the aimed resource allocation of the National Cyber Security Programme between 2011 and 2015. The highest allocation was directed to “Single Intelligence, Account, building cross cutting capabilities, including Information Assurance” (59%), followed by the “Ministry of Defence, mainstreaming cyber in defence” (14%) (CABINET OFFICE, 2011, p. 25).

Another structural change in 2011 was the shift of ministerial responsibility for cybersecurity from the Home Office to the Cabinet Office (NAO, 2013, p. 10). With the budget and cyber institutional framework re-organized, one must note that the UK's cyber institutional framework was designed with a centralized nature. Furthermore, despite the heavy intelligence component, the 2011 NCSS balanced security with freedom and privacy, along with the risk-based approach and partnership (CABINET OFFICE, 2011, p. 24).

The 2011 NCSS also took a step further by describing the UK's actions to tackle cyber threats, adding a "how" element to the Strategy. Among the priority actions were: the improvement of detection and analysis of cyber threats, pool knowledge and situational awareness, enhancement of defense and deterrence capabilities, development of international principles for behavior in cyberspace, persuasion of other countries to develop compatible laws to the Budapest Convention[25], use of cyber relevant sanctions to tackle cyber crimes and creation of a thriving market in cyber security products and services (CABINET OFFICE, 2011, p. 26).

From the launch of the 2011 NCSS on, the UK Government would annually assess the progress on the action implementation, consolidating its digital mentality even further. In this context, the Olympics in 2012 had a significant impact on the country, as it "provided a genuine test of our [the UK] preparedness with potential threats successfully averted" (CABINET OFFICE, 2012a, p. 5). Moreover, the Cabinet Office, security and Intelligence Agencies, and other departments and agencies established "unprecedented mechanisms for working hand in hand with sponsors and suppliers to the Games in handling and combating cyber threats" (CABINET OFFICE, 2012b, p. 3).

Beyond the Olympic Games, it is relevant to point out that the MoD established a Joint Cyber Unit hosted by the GCHQ (CABINET OFFICE, 2012b, p.3). Also, a "Cyber reservists" program for the MoD was planned to be put forward. Establishing a National Cyber Crime Unit as an integral part of the National Crime Agency was externalized. The private-public sector information sharing "hub" pilot was completed, and the first eight "Academic Centres of Excellence in Cyber Security Research" were defined.[26] (CABINET OFFICE, 2012a, 2012b).

Still, in 2012, some ideas raised in the 2011-2012 ISC report indicated the direction the UK's digital mentality would take in the following years. The report highlighted the following cyber threats: crime, terrorism, and other nation-state espionage, pointing specifically to China and Russia. Besides, it indicated that the Committee believed some opportunities should be, including active defense, exploitation, disruption, information operations, and military effects (ISC, 2012, p. 36). Despite the present, these ideas would need to evolve within UK's mentality. From the 2011 NCSS, the country perceived itself as a consolidating "digital economic power," The document's focus still followed a market orientation, despite broadening up actions and aimed results.

The foreign secretary's speech at the Budapest Conference on cyberspace reinforces the market approach. He said the UK was determined to be a world leader in cyber security,

[25] The UK ratified the Budapest convention, also known as the Convention on Cybercrime, in 2011 (COE, 2022).

[26] The GCHQ, in partnership with the Engineering and Physical Sciences Research Council and the Department for Business Innovation and Skills, awarded the title of Academic Centres of Excellence in Cyber Security Research to eight UK universities. The eight centers were: University of Bristol, Imperial College London, Lancaster University, University of Oxford, Royal Holloway University, Southampton, Queens University Belfast, and University College London (CABINET OFFICE, 2012a. p. 8).

.

and the government wanted the UK to be a "pre-eminent safe space for e-commerce and intellectual property online" (FCO; HAGUE, 2012). It also reinforced the idea of building a foundation on the “rules of the road” for cyber behavior (going beyond crime and state-sponsored cyber attacks) since the speech mentions as a factor to states come together: the growing divergence of opinion and action between those countries seeking an open future for the Internet and those who are inching down the path to state control" (FCO; HAGUE, 2012). This type of statement clearly set the boundaries between the "other" and the "self" by an economic perspective. The open versus closed Internet intertwines with the idea of the free flow of data, the base for the digital economy.

In 2013 a new review of the 2011 NCSS was done. The statement of Francis Maude of the Cabinet Office on the strategy's progress pointed to an investment increase for the National Cyber Security Programme of a further £210 million from 2015 to 2016 (CABINET OFFICE; MAUDE, 2013). Besides the documents produced, one toward the forward plans and the other the progress of objectives, highlighted many developments. Among the developments, it is relevant to highlight the ones contributing to the country's digital mentality, such as:

a) The launch of the Cyber Security Information Sharing Partnership (CISP) (which fostered an environment for the exchange of cyber threat information in real-time, especially among critical infrastructure providers);
b) The design of a national CERT (CERT-UK);
c) The Center for the Protection of National Infrastructure (CPNI) focuses on protecting Critical National Infrastructure from insider threats;
d) The Defence Cyber Protection Partnership (DCPP) (aimed to improve the defense supply chain);
e) The Join forces cyber group (comprised of the Joint cyber Units at Cheltenham and Corsham and the "Cyber Reserve," Joint Cyber Unit) and the addition of three new Academic Centers of Excellence in Cyber Security Research[27] (CABINET OFFICE, 2013a; 2013b).

These developments show a concern with stepping up at least defense capabilities. However, this does not mean that offensive capabilities were not aimed. In 2013 Philip Hammond, the defense secretary at the time, stated ahead of the Conservative party conference in Manchester that the UK was developing military cyber capability, including a

[27] Birmingham, Cambridge and Newcastle (CABINET OFFICE, 2013b).

strike one (BLITZ, 2013). Thus, one can assume that the ideas observed in the 2011-2012 ISC report were already shaping UK's digital mentality.

As the first nation to publicly state the development of offensive cyber capabilities (BLITZ, 2013) and after the Snowden revelations,[28] The UK's international image as a trustworthy partner suffered a shock. Thus, the ISC investigated allegations made in the media of improper content communications access by GCHQ through the NSA's PRISM[29] capability and issued an early statement concluding that the allegations were "unfounded" (ISC, 2013a; ISC, 2014). Besides, the 2012-2013 ISC report emphasized that "despite the increased profile of other threats such as cyber security, counter-terrorism work rightly remains the primary focus of the intelligence and security Agencies." The report indicated that ISC supported the "Government's efforts to raise awareness and, more importantly, our nation's defences" (ISC, 2013b, p.47).

The 2014 NCSS review combined the plans forward and the progress of the objectives in one document. This document highlighted a series of activities, among them:

a) The launch of the UK's National Computer Emergency Response Team (CERT-UK).
b) The progress in tackling cybercrime through the international engagement of the National Cyber Crime Unit.
c) The development of a Cyber Security Model of Defence, designed to be a framework of expected cyber standards (to be implemented in 2015).
d) The introduction of cyber Essentials, which set basic standards of cyber security for UK organizations.
e) The expansion of the UK's bilateral and multilateral networks, including EU and NATO, this last one with the UK becoming a full member of the NATO Cooperative Cyber Defence Centre of Excellence (CABINET OFFICE, 2014).

Besides these developments, the 2013-2014 ISC report highlighted that in addition to the expenditure, administration, policy, and operation of intelligence and security agencies, it agreed with the government to oversee activities from the MoD and Cabinet Office, including offensive cyber and activities of the Joint Intelligence Organisation[30] (ISC, 2014).

[28] The Snowden revelations refer to the leak made by Edward Snowden, a former American intelligence contractor, of top-secret documents revealing a vast intelligence capacity of GCHQ to capture communications. This episode triggered an international debate over digital privacy and the proper limits of the intelligence services' intrusive capabilities (UK PARLIAMENT, 2022).

[29] PRISM was a program that allowed officials to collect material including search history, the content of emails, file transfers and live chats (GREENWALD; MACASKILL, 2013).

[30] "The Joint Intelligence Organisation leads on intelligence assessment and development of the UK intelligence community's analytical capability, supporting the work of the Joint Intelligence Committee and National Security Council" (UK GOVERNMENT, 2022).

The developments of 2014 showed the sedimentation of a government's more proactive actions toward cyberspace and cybersecurity and the careful consideration of transparency within the intelligence and security Agencies. This sedimentation was further explicit in the National Security Strategy (NSS) and Strategic Defence and Security Review (SDSR) 2015.

The NSS/SDSR 2015 continued to place cyber as a Tier One priority risk for the UK. One of the challenges likely to drive UK priorities was the "impact of technology, especially cyber threats; and wider technological developments" (HMG, 2015, p. 15). In this sense, it set as one of the priorities for the UK in a five-year time frame to "remain a world leader in cyber security" and "deter state-based threats" (HMG, 2015, p. 10). The document also reinforced the view of cyber threats through criminals, terrorists, and states, highlighting that the UK would treat a cyber attack as seriously as it would do with a conventional attack and that "we [the UK] will defend ourselves as necessary" (HMG, 2015, p. 24).

In this context, the NSS/SDSR 2015 indicated the UK would develop the necessary components to defend itself from a cyberattack, including

> (…) capabilities that allow us to understand and tackle the most advanced threats, law enforcement capabilities to deal with cyber crime, support for business, particularly in the UK's CNI [Critical National Infrastructure], and the skills and innovation for the long term (HMG, 2015, p. 40).

Besides, it exposed that cybersecurity contributed £17 billion each year to the UK's economy and recognized some strategic partnerships involving cyber more deeply, among them with the USA and Germany. Finally, it also stressed that 1.2% of the defense budget would be dedicated to science and technology and, as part of the £165 million Defence and Cyber Innovation Fund, it would increase funding "to support the procurement of innovative solutions to the challenges facing Armed Forces" (HMG, 2015, p.74).

Regarding the 2015 NSS/SDSR review, it is important to stress that the impacts of the Snowden revelations led to further developments regarding UK's balance between privacy and security. In March 2015, the ISC published a report on the full range of intrusive capabilities the intelligence and security Agencies had to protect the country. Moreover, it recommended the UK take a more transparent approach, as much as possible, toward intelligence and security Agencies. According to the report:

> **The Committee has identified several areas where we believe there is scope for the government to be more transparent about the Agencies' work. The first step – as previously set out – is to consolidate the relevant legislation and avow all of the Agencies' intrusive capabilities. This will, in itself, be a significant step**

> **towards greater transparency. Where it is not practicable to specify the detail of certain arrangements in legislation, the government must nevertheless publish information as to how these arrangements will work (for example, in Codes of Practice).** (ISC, 2015, p. 109).

All the elements highlighted in the documents point to 2015 as the prelude to a change in UK's digital mentality. This change would later be solidified in the next NCSS.

3.1.2 The second phase (2016-2021): Government-Driven approach

The 2016 NCSS not only planned a budget of £ 1.9 billion to be spent within the five-year Strategy time frame but also, and already in its forward, expressed to be “an unprecedented exercise of transparency” (HMG, 2016, p. 6). In this sense, the Strategy innovated by providing a more government proactive approach, setting the vision for 2021 for the UK to be "secure and resilient to cyber threats, prosperous and confident in the digital world."

The 2016 NCSS explained that a comprehensive approach would be required to effectively secure cyber interest, which would mean engaging citizens, industry, and other partners in society and government. Still, despite a holistic approach, it was explicit that the government would take the lead. Among other assessments, the UK realized.

> a market based approach to the promotion of cyber hygiene has not produced the required pace and scale of change; therefore, Government has to lead the way and intervene more directly by bringing its influence and resources to bear to address cyber threats (HMG, 2016, p.13).

In this context, the NCSS set three main objectives: deter, defend and develop, having the pursuit of international action as an underpinning element. These objectives can be interpreted parallel to conventional power ideas involving diplomatic, military, economic, and informational power.

Despite the continuity in the perception of some conventional power elements, the 2016 NCSS set a heavy tone on offensive and defensive capabilities development. Using active cyber defense and offensive cyber capabilities translates this element. According to the Strategy, "Active Cyber Defence (ACD) is the principle of implementing security measures to strengthen a network of systems to make it more robust against attack" (HMG, 2016, p. 33). Thus, ACD was placed within the defend objective of the NCSS. While the offense was set along the deter objective of the Strategy, since “Offensive cyber forms part of the full spectrum of capabilities we will develop to deter adversaries and to deny them opportunities to attack us, in both cyberspace and physical sphere" (HMG, 2016, p. 51). Thus, the UK would encompass the development of such capabilities within a National Offensive Cyber Programme (NOCP). Moreover, it is relevant to point out that offense and cryptography were out together as sovereign capabilities to be enhanced by the Strategy. This also points to the concern with cyber espionage and can be understood as an exposition on using deterrence by denial.

The express mention of the development of defense and offense capabilities coupled with the Snowden revelations repercussion and the preference of the UK for using intelligence agencies heavily in the cybersecurity mix generated new legislation aligned with the ISC's previous recommendations: The Investigatory Powers Act (IPA). Therefore, IPA describes and expands the electronic surveillance powers of the intelligence agencies, rendering these more transparent and with more significant safeguards on their use, including judicial review and warrants (STEVENS, 2021a, p. 195). Thus, the legal framework was in alignment with the new NCSS. The cyber institutional framework of the UK would also receive some attention. The 2016 NCSS also proposed the creation of the National Cyber Security Centre "to be the authority on the UK's cyber security environment, sharing knowledge, addressing systemic vulnerabilities and providing leadership on key national cyber security issues" (HMG, 2016, p. 10).

Regarding threats, the 2016 NCSS reinforced the idea of threats coming from cyber criminals, states, state-sponsored groups, terrorists, and hacktivists. Still, the Strategy added a new category of threat: script kiddies[31], despite being labeled as not assessed as a substantive threat, highlighted that "the actions of 'scrip kiddies' can, in some cases, have a disproportionately damaging impact on an affected organisation" (HMG, 2016, p. 20). Notwithstanding, it calls attention to the highlight given to "insiders." The 2016 NCSS describes two types of insiders who act intentionally and unintentionally. In this sense, and with all the Snowden repercussions, the Strategy puts as the highest threat malicious insiders, meaning "trusted employees of an organisation and have access to critical systems and data, [...] They can cause financial and reputational damage through the theft of sensitive data and intellectual property" (HMG, 2016, p. 19).

On the development objective, the 2016 NCSS stressed that a "skilled workforce is the lifeblood of a vital and world leading cyber security commercial ecosystem" (HMG, 2016, p.

[31] Script kiddies only use existing software to launch an attack, not having the skills or will to develop attack tools by themselves

55). In this sense, and among other actions, the UK committed itself to develop a Defence Cyber Academy across the Ministry of Defence and wider Government as a center for cyber training and exercises. Besides the Strategy set as a goal to straighten the UK's position as a world leader in cyber science and technology, one of the steps toward this goal would be publishing a detailed Cyber Science and Technology Strategy[32] (HMG, 2016). Moreover, the Annual Review of the NSS/SDSR summarizes some crucial efforts, such as the CyberInvest (that in 2016 had 25 industry members investing in cyber security research at UK Universities), the 13 recognized university Academic Centres of Excellence in Cyber Security Research, and the investment of GCHQ in 3 research institutes to develop capabilities in strategical areas (CABINET OFFICE, 2016, p. 28).

On international action, it reinforced the role of building the "rules of the road" for behavior in cyberspace. In the international arena, the Strategy explains that the UK would seek to "influence the decision-making of those engaging in cybercrime, cyber espionage, and disruptive or destructive cyber activity and continue to build frameworks to support international cooperation" (HMG, 2016, p. 63). Moreover, more attention on bilateral and multilateral forums continued, focusing multilaterally on forums like the UN, NATO, G20, European Union, OSCE, Council of Europe, and Commonwealth. Besides, the Annual Review of the NSS/SSDR stressed the relationship with China. According to the document, a UK-China Security dialogue occurred in June 2016, and the countries agreed on further collaboration on several topics, including cyber (CABINET OFFICE, 2016, p. 23).

All the objectives and action proposals on the 2016 NCSS indicate a self-identity centered on a leadership role. The NCSS stated that the UK was a world leader in cyber security (HMG, 2016, p.13; p. 38) and stressed its ambition to be a leading digital nation (HMG, 2016, p. 37). Thus the 2016 NCSS reinforced the “notion of the UK as a dynamic, outward-facing entrepôt nation and the potential of the cybersecurity industry itself to become a vibrant economic sector” (STEVENS, 2021a, p. 192). A vision that can also be seen in the Annual Review of the NSS/SDSR when it explains, "We [The UK] are delivering a comprehensive cyber security business engagement strategy to help industry protect itself in cyberspace" (CABINET OFFICE, 2016 p. 15).

One year after the launch of the NCSS, two major cyber attacks impacted the UK: Wannacry and NotPetya. On 12th May 2017, WannaCry, global ransomware, affected over 200,000 computers in at least 100 countries, one of them being the UK. Specifically, it

[32] The Interim cyber security science and technology strategy was published in 2017.

affected the UK's National Health Service (NHS), with about 80 of 236 NHS trusts suffering disruption across England (HOUSE OF COMMONS, 2018). It only stopped because a cyber-security researcher activated a kill switch, so the malware stopped locking devices. NotPetya was also global ransomware, but it diverged from Wannacry. Even if the victims paid the ransomware, it was coded so the stolen data could not be returned. NotPetya hit 2,000 users in Russia, Ukraine, Poland, France, Italy, the UK, Germany, and the USA. Both malware resulted from hacking the NSA's toolbox of hacking techniques. The hack resulted in the release of details of a weakness in Microsoft's Windows operating system that could be used to run programs on other computers on the same network automatically, code-named Eternal Blue (HERN, 2017; HELEN; SOLON, 2017).

After the malware's impact, the UK started implementing an attribution practice, which was previously set as a possibility to stop hostile foreign action in cyberspace in the 2016 NCSS. (HMG, 2016, p. 50). In December 2017, the UK and its allies attributed the Wannacry cyberattack to North Korean actors. In February 2018, the UK and 12 partners attributed the NotPetya cyber-attack to the Russian military. In October 2018, the UK, with 19 partners, the EU, and NATO, attributed a global campaign of cyber attacks targeting political institutions, businesses, media, and sports to Russian military intelligence. In December 2018, the UK, with 14 partners, attributed a campaign of malicious cyber activity targeting intellectual property and sensitive commercial data in Europe to APT 10, a hacking group acting on behalf of the Chinese Government (CABINET OFFICE, 2019, p. 18).

This practice led to the promotion by the UK and Netherlands of a cyber sanctions regime within the EU, and in 2019 the Council of the European Union adopted Council Decision (CFSP) 2019/797 and Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. (BOTEK, 2019) With the introduction of the cyber sanctions regime, the UK adopted such a regime as a Member State. As a Member State of the EU, the UK also adopted the Data Protection Act of 2018[33]. As a consequence of the European Union's General Data Protection Regulation (GDPR), it implemented the 2016 EU Directive on the security of network and information systems (NIS Directive), which "identifies essential operators of UK information infrastructure and incentivizes better cybersecurity" (STEVENS, 2021a, p.195).

[33] It is important to highlight that the UK had previous legislation on data protection, such as the Data Protection Act (1998) and Electronic Communications Regulations (2003), but the Data Protection Act (2018) tightens up the data protection framework (STEVENS, 2021a, p.195).

Besides the legislative upgrade, the UK also exposed its offensive capabilities implementation parallel to a military campaign for the first time.[34]In partnership with MoD, the GCHQ deployed offensive capabilities against the Islamic State group[35] disrupting the group's online activities and even destroying equipment and networks (BBC NEWS, 2018). In this sense, 2017 and 2018 were marked with evidence of the implementation of the 2016 NCSS since the Strategy also pointed out that the UK has “the means to take offensive action in cyberspace” should it choose to do so (HMG, 2016, p. 9).

Another relevant aspect of the UK's digital mentality between 2017 and 2019 was its perception regarding "fake news" and the cyber skills gap. National Security Capability Review (CABINET OFFICE, 2018) acknowledge the discard of traditional media in favor of digital and social media platforms and the use of communications by adversaries to achieve a strategic advantage. According to the document, "The democratisation of information, and the means to exploit it, has allowed hostile actors to exert disproportionate influence in competition with public interest" (CABINET OFFICE, 2018). Thus, in the general elections of 2019, the UK expressed its approach to safeguarding elections (CABINET OFFICE, 2019, 16).

The concern related to elections, despite not explicitly associated with the term "fake news," was already put in place in 2017, as the 2016-2017 ISC report indicated that UK's political system was "a potential target for cyber attacks by hostile foreign states and terrorist groups" (ISC, 2017, p. 32). Also, the 2017-2018 ISC report indicated that the Committee worked closely with the NCSC to mitigate potential threats to the 2017 General Election (ISC, 2018, p. 16). This perception was reactive to Russian interference in the 2016 US presidential election (ISC, 2017, p. 33). In this regard, an increasing concern with critical infrastructure protection was stated

> **The combination of the high capability of state actors with an increasingly brazen approach places an ever greater importance on ensuring the security of systems in the UK which control the Critical National Infrastructure. Detecting and countering high-end cyber activity must remain a top priority for the Government** (ISC, 2017, p. 32).

Building on these concerns, the UK worked in 2019 to continue the ACD program to make infrastructures, products, and services "automatically safer and easier to use by

[34]In 2016 the then Defence Secretary confirmed the UK was conducting cyber operations against Daesh. In 2018, Director GCHQ revealed how it had degraded ISIS propaganda networks through cyber operations (GCHQ, 2020). It is also worth noting that a cyber doctrine for the military already existed. In 2016 the second edition of Cyber Prime was launched (MOD, 2014).

[35]Also known as Daesh

organisations" (CABINET OFFICE, 2019, p.16). Also, it continued the work that began in 2018 to deliver an "Initial National Cyber Security Skills Strategy" (CABINET OFFICE, 2019, p. 47).

Besides these developments, the speech of the GCHQ Director, Jeremy Fleming, on two occasions in 2019, was a good indication of the nation's thinking over the term cyber power. In February 2019, at the Fullerton Lecture at the International Institute of Strategic Studies in Singapore, Mr. Fleming spoke that a new lexicon was needed, “One that isn’t based on the overly military language of past power frameworks, but a language that clearly refreshes and restates for the cyber age the underlying principles that have served our democracies so well for hundreds of years” (FLEMING, 2019a, p. 2). In this sense he indicated that dialogue involving Cyber power should understand the concept beyond the Internet and technology. Thus he stated that for him “a Nation is a Cyber Power if it is able to direct or influence the behaviour of others in Cyber space” (FLEMING, 2019a, p. 4) and three ways could achieve this influence:

> One - it must be world-class in safeguarding the cyber health of its citizens, businesses and institutions - it must protect the digital homeland.
>
> Two - it must have the legal, ethical and regulatory regimes to foster public trust - without which we just don't have a licence to operate in cyber space.
>
> And three - when the security of the nation is threatened, it has to have the ability - in accordance with international law - to project cyber power to disrupt, deny or degrade our adversaries (FLEMING, 2019a, p. 4).

In this sense, cyber power would have defensive, offensive, and normative elements, the same ones under consolidation in UK’s digital mentality.

In Mr. Fleming's speech, he also stressed the need for action to meet "legality, necessity and proportionality" and the relevance of making alliances and cooperating internationally. In this sense, he said, "I believe the UK is a Cyber Power with the potential to provide leadership in this debate." and that "GCHQ is at the heart of that" (FLEMING, 2019a, p. 17). In his last speech, in April 2019, at the NCSC's flagship cyber security event, CYBERUK 2019, he reinforced the idea of the cyber power elements. He stressed "how significant cyber security is becoming to a nation's cyber power."(FLEMING, 2019b, p. 8). Despite the speeches, no official open-source document mentioned cyber power. However, the seed of the concept was planted, and the UK's position on leaving the EU would prefer immediate cyber reasoning.

With the UK leaving the EU in 2020 (Brexit), it adapted its legislation to continue with the logic of the cyber sanctions regime, and the Cyber (Sanctions) (EU Exit) Regulations 2020 came fully into force on 31st December 2020 (FCDO, 2020). The same happened regarding the NIS Directive. The adaptation of the NIS Directive resulted in the Information Systems (EU Exit) (Amendment) Regulations 2021, coming into force in 2022 (DATA GUIDANCE, 2022). The same also happened with GDPR, resulting in the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019 (the "UK GDPR") coming into effect in 2021 (INFORMATION COMMISSIONER'S OFFICE, 2022). However, more remains to be seen regarding cybersecurity operational effectiveness. Stevens (2021b) pointed out that Brexit introduced “uncertainty into a number of areas important to security and policing, and exclude the UK from EU cybersecurity decision-making." Brexit has not drastically affected the UK's digital mentality despite these operational issues. Events in the following years, amid the COVID-19 pandemic, would consolidate some practices and even modify some perceptions.

The COVID-19 pandemic brought a proliferation of cybercrime and raised international attention to espionage and critical health infrastructure vulnerabilities to cyber-attacks. In this context, in November 2020, the UK created the National Cyber Force. The National Cyber Force (NCF) was designed to bring together personnel from GCHQ, the MoD, the Secret Intelligence Service (MI6), and the Defence Science and Technology Laboratory (DSTL) under one unified command. It aims to conduct cyber operations to disrupt the perceived usual threat actors (hostile foreign actors, criminals, and terrorists) to UK's national security (ISC, 2021). It was the first step in the reasoning, followed by the Integrated Review launched in 2021.

The Integrated Review of Security, Defence, Development, and Foreign Policy is a comprehensive document that sets the UK's defense and strategic security direction for the next ten years. Within its structure, a Strategic Framework establishes the UK's national security and international policy objectives with priority actions to 2025 and all the goals to encompass a cyber element. Specifically, the framework sets four objectives:

a) Sustaining strategic advantage through science and technology.

b) Shaping the open international order of the future.

c) Strengthening security and defense at home and overseas.

d) Building resilience at home and overseas

In this regard, it calls attention to the term cyber power in the official document. The first objective explains that the use of S&T will be incorporated as an 'integral element" of national security and international policy, "fortifying the position of the UK as a **global S&T and responsible cyber power**” (HMG, 2021a, p. 18). The document further explains the UK aims to "**grow the UK’s science and technology power in pursuit of strategic advantage**," and "**cement the UK’s position as a responsible and democratic cyber power, able to protect and promote interests in and trough, cyberspace**."(HMG, 2021a, p. 35) In this regard, the UK considers cyber power as the

> […] the ability to protect and promote national interests in and through cyberspace: to realise the benefits that cyberspace offers to our citizens and economy, to work with partners towards a cyberspace that reflects our values, and to use cyber capabilities to influence events in the real world (HMG, 2021a p. 40).

Moreover, the Integrated Review describes that:

> Cyber power protects our national security and the resilience of our CNI. It supports economic growth, enabling businesses and individuals to transition confidently to the digital world, boosting productivity and driving the innovation that will create new skilled jobs. It also creates new ways to pursue and protect our interests, enabling us to detect, deter and disrupt our adversaries in cyberspace and on the ground, and to influence the global environment to ensure a safe and beneficial digital future for all (HMG, 2021a, p. 40).

This definition recalls the elements of cyber power in the GCHQ's director speech in 2019, also setting cyber security as its foundation. However, it highlights that instead of having a primary cybersecurity focus on the strategical level, the new cyber Strategy would be comprehensive, adopting a "whole-of-cyber" approach[36] to be overseen by a small ministerial group to cohere decision making across the government (HMG, 2021a, p. 40).

Five priority actions within this larger S&T objective were set.

a) To strengthen UK’s cyber ecosystem, meaning more integrated and coherent actions involving cyber actors in government, academia, industry

b) to build a resilient and prosperous UK, meaning the transformation of the UK's digital economy and protection of CNI and the private sector from cyber attacks

[36] “(…) that considers the full range of our capabilities and gives greater weight to building advantage in critical cyber technologies, as well as to international action to influence the future of cyberspace” (HMG, 2021a, p. 40).

c) to take the lead in technologies vital to cyber power, meaning the development of technologies such as microprocessors, secure system designs, quantum technologies, and new forms of data transmission
d) to promote free, open, peaceful, and secure cyberspace, meaning straightening the UK as a cybersecurity leader and broader international partnerships (both to share values and uphold international norms)
e) to detect, disrupt and deter adversaries, meaning a more “integrated, creative and routine use of UK’s full spectrum” – diplomatic, military, intelligence, economic, legal and strategic communications tools, besides NCF – "to impose costs to our adversaries, deny their ability to harm UK interests, and make the UK a more difficult operating environment" (HMG, 2021a, p. 41).

In this regard, it is interesting that the idea of "cyber power" is not detached from the conventional elements of power and that the "agenda-setting" element, translated by "influence," balances an idea of soft and hard power. It reminds a modification of Nye's cyber power concept. The influence is so present in the concept that the Integrated Review calls attention to cyber diplomacy as a "critical element" of cyber power (HMG, 2021a, p. 45) and the idea of strengthening capacity and cooperation with like-minded partners (HMG, 2021a, p.75). While a resemblance of hard power could be seen in the broader objective three, when the Integrated review mentions a "more robust approach," improving the UK's ability to detect, disrupt, defend and deter the threats we face in the physical world and in cyberspace" (HMG, 2021a, p. 69).

The reasoning of S&T as a metric for cyber power and the emphasis on cyber security was also translated to the MoD Digital Strategy for Defence (DSD), launched in April 2021. The Digital Strategy for Defence set importance on securing the UK's Digital Backbone (a combination of people, processes, data, and technology), which would require a transformation of the UK's approach to defensive cyber security. The DSD was designed to set the UK’s defense vision for 2030, pointing out that Data will be a strategic asset and the need for alignment with UK's ambition to become a recognized global cyber power (MOD, 2021). Both documents paved the way for the 2022 NCSS, published in December 2021.

3.1.3 The third phase (2022 - ...): Global approach

The new NCSS set the UK's 2030 vision for the country "to continue to be a responsible and democratic cyber power, able to protect and promote our [the UK] interests in and through cyberspace in support of national goals." The 2022 NCSS retained the Integrated Review's definition of cyber power, stressing three important conclusions reached by the Integrated review:

a) that cyber power will be an ever more important lever to delivering the UK's goals,

b) that sustaining cyber power would require a more comprehensive and integrated strategy, and

c) a whole of society approach is needed (HMG, 2021b, p. 11).

In this regard, one can infer the UK started to think with a truly global approach, going away from the centrality of the government. Notwithstanding, cyber power is perceived as something to acquire, retain and expand, a characteristic of the conventional concept of "power over,” thus still having a solid government element.

The 2022 NCSS also builds on the five pillars and priority actions of the Strategic Framework drawn in the Integrated Review, explaining them more profoundly. The NCSS also details cyberspace, its layers (physical, logical, and virtual), the UK's concept of cyber power, and the country's self-perception as a leading cyber power. The Strategy explains that evidence of the UK's leading cyber power can be found in the ITU Cybersecurity Index, Harvard's Belfer Center's Cyber Power Index, and the Strategy Studies's Cyber Power capability net assessment. This point shows how publication on cyber power also affects a country's self-perception and surrounding environment, reinforcing the idea of a co-creation evolution.

On the Cyber Power concept itself, the 2022 NCSS points to five broad dimensions in alignment with the pillars of the Strategy. These dimensions are:

a) The people, knowledge, skills, and partnerships considered the foundation of the UK's cyber power

b) The ability to protect assets through cyber security and resilience

c) The technical and industrial capabilities

d) The global influence, relationships, and ethical standards, for shaping the rules and norms of cyberspace

e) The ability to take action in and through cyberspace to support national security, economic well-being, and crime prevention

Concerning the last point, the 2022 NCSS explains that this ability to take action includes cyber operations "to deliver real world effect, and to help achieve strategic advantage, and law enforcement operations and the application of cyber sanctions to bring malicious cyber actors criminals to justice and disrupt their activities" (HMG, 2021b, p. 20). The documents further explain that the "UK's approach to build its cyber power has included concerted efforts to develop the country's cyber skills base and commercial capabilities" (HMG, 2021b, p. 21). Thus, the development of 19 Academic Centres of excellence and four research institutes tracking cyber security challenges.

Through the 2022 NCSS, some other aspects are worth stressing, as they provide a better picture of how the UK perceives cyberspace and its threats. The usual cyber actors' threat landscape was maintained: criminals, terrorists, hostile foreign actors, and activists (hacktivists). However, special attention was given to ransomware and supply chain attacks [37], as well as disinformation, sabotage, and espionage. Besides, the NCSS indicated that cyberspace would become more contested. Thus, the relevance of cyber operations to "power projection below the threshold of armed conflict and pre-conflict situations" (HMG, 2021b, p. 30). Besides, the competitive advantage of the UK would come from the UK's ability to " nurture and harness talent across the UK and get the right people working together in the right ways across the whole public sector, industry and academia" (HMG, 2021b, p. 50). In other words, the use of a "whole of a society approach."

Another relevant aspect is among the pointed shifts the Strategy brought into UK's strategic perspective. Thus, it calls attention to the NCSS, putting "cyber power at the heart of the UK's foreign policy agenda recognising that every part of the strategy requires international engagement" (HMG, 2021b, p. 36). This shift reinforces the idea of power projection by focusing on cyber capacity building (CCB)[38] development worldwide. It also recalls the UK's idea of cyber resilience, which is explained to be made of three key aspects: a) the need for the nature of the risk to be understood, b) the need for action to secure systems to prevent and resist to cyber-attacks and c) be resilient enough to minimize impacts and being able to recover (HMG, 2021b, p. 65). In this sense, recognizable allies are essential to the UK[39], especially as another shift is "more integrated and sustained campaigns to disrupt and

[37] The document pointed to the UK's action toward attribution to global cyber attacks such as SolarWinds and Microsoft Exchange (HMG, 2021b, p. 25) and used both cases as examples of "states exploiting strategic vulnerabilities and supply chains" (HMG, 2021b, p. 27).

[38] According to the 2022 NCSS, the UK will prioritize CCB in Eastern Europe, Africa, Indo-Pacific and continue to work with key allies in the Americas and the Middle East in this regard (HMG, 2021b, p. 992).

[39] According to the 2022 NCSS, the UK will "continue to work with effective multilateral organisations and partnerships, including the United Nations, Five Eyes, NATO, G7, European Union, Commonwealth, OECD,

deter our adversaries and protect and promote the UK's interest in cyberspace" (HMG, 2021b, p. 36). In other words, meaning a more robust use of attribution and offensive capability, this last one materialized through the new NCF.

Despite the explicit use of defensive and offensive cyber capabilities, it is interesting to note the stress given to the UK being a responsible and democratic cyber power. These two adjectives were translated as acting lawfully and proportionally, securing an open and free Internet (HMG, 2021b). This indicates the UK built upon previous experiences of lack of transparency (Snowden revelations) and reinforced its commitment to discovering how international law applies to cyberspace, as the country has confirmed its applicability to cyberspace since 2015.

A final remark to the 2022 NCSS is a preference to center intelligence at the heart of cyber actions and its perception of cyber espionage. These elements were transposed to the NCSS as one of the objectives within the pillar "Taking the lead in the technologies vital to cyber power," which involved Crypt Key. The objective is "to preserve a robust and resilient national CryptKey enterprise which meets the needs of HMG customers, our partners, and allies, and has appropriately mitigated our most significant risks, including the threat from our most capable adversaries" (HMG, 2021b, p.85). "Crypt-key is the term used to describe the UK's use of cryptography to protect its critical information and services." But more relevant is that the UK will maintain its "leadership role in the Five Eyes, NATO and other international partnerships" to make UK’s Crypt-Key solutions to be interoperable and work with industry to maximize export opportunities (HMG, 2021b, p. 85).

3.2 CYBER POWER PERCEPTIONS

As the analysis of the documents and the relevance of external impacts showed, the UK evolved its digital mentality to the point that it perceived itself as a leading cyber power. With this mentality development, the concept of cyber power and being a cyber power became more straightforward for the country. Still, its digital mentality affects its perceptions, forming its situational awareness and own definition of cyber power. A summary of the UK's digital mentality evolution and the importance of the theme for the country can be seen in Table 9.

Global Forum on Cyber Expertise (GFCE), ASEAN Forum, African Union and the World Bank" (HMG, 2021b, p. 93).

Notwithstanding the documents, in the pursuit of interviews, I could apply the semi-structured questionnaire to a cyber diplomat from FCDO. The contact with organizations such as NCSC resulted in a negative answer to the questionnaire application. In contrast, despite not providing direct answers to the questionnaire, the contact with the MoD gave some guidance in crucial documents.

From the interview with a cyber diplomat, it is worth mentioning the answer on the impact of cyber on the international system. The documents pointed to an idea of polarization between an open and free Internet and a closed one, with greater state control. In this sense, the interviewee said it was "not about hierarchy but a sort of polarization" (INTERVIEWEE A, 2020). The interviewee explained that polarization could be seen in attempts to create new protocols for Internet functioning, the proposal of an international cybercrime treaty in opposition to the Budapest Convention, and the discussions over a free and open Internet in contrast to a more state-controlled one. Besides, the interviewee emphasized that because of the growth of an interconnected economic space and the increase of attack surface for cyber-attacks, national power, and cyber power could not be detached, especially if one thinks about the need for economic security and domestic resilience (INTERVIEWEE A, 2020).

Table 9 - UK's Digital Mentality Summary

NCSS	Orientation	Threats Perceived	Self Perception	Investment	Conventional Power Elements
2009	Market-driven approach	Criminals (e-crime) Terrorists States and patriotic hackers (espionage, influence, warfare)	Emerging digital Economic Power	£ 650 million	Economic, military, informational
2011	Market-driven approach	Criminals States and patriotic hackers (foreign intelligence services and military) Terrorists Hacktivists	Consolidating Digital Economical Power	£ 860 million	Economic, military, informational, and diplomatic
2016	Government driven approach	Criminals (cyber-dependent and cyber-enabled crimes) State and State-Sponsored (espionage, offensive cyber capabilities) Terrorists Hacktivists Insiders Script Kiddies	Cyber security leader and digital economic power	£ 1.9 billion	Military, informational, economic, and diplomatic

2022	Global approach	Criminals States/State-based actors Activists Terrorists * Special attention is given to ransomware and Supply Chain attacks, Disinformation, Sabotage, and Espionage	Leading Cyber Power	£ 22 billion	Military, economic, diplomatic, informational, and institutional

Source: Own elaboration based on UK’s National Cyber Strategies.

Also interesting was that the answer around some elements of cyber power that was later on displayed in the 2022 NCSS, such as "CNI protection," "resilience," "cyber signals" capability (meaning capable intelligence agencies), "innovative private sector," "diplomatic infrastructure" and "horizon scanning." According to the interviewee, "being in the top [discussions] table is critical" for power projection. These tables would be within the UN's first and third committees, ITU, OEWG, and OECD. Moreover, according to the cyber diplomat, to maintain one's cyber power, it would be necessary to build coalitions (bilaterally and multilaterally) and have "innovation credibility." In sum, to acquire and maintain cyber power, it would be important to think about "economic security," "economic resilience," and thus "how cyber power and defense capabilities can be best used to defend one's economy"(INTERVIEWEE A, 2020). In this regard, one can observe that the dual engine of the UK's thinking: cyber security and economy, reverberates at the individual level of agents.

The interviewee's view on the term cyber power was also relevant. The interviewee said, "the notion of cyber power has been around for quite some time, but the label is currently being debated"(INTERVIEWEE A, 2020). Indeed, the UK was one of the first to openly use the term in official documents. Besides, the cyber diplomat indicated that thinking about future risks would be equally important, thus the need for a good "horizon scanning" capability. In other words, the ability to perceive potential risks and opportunities in emerging technologies.

The interviewee's view on cyber power can be summarized in a short sentence at the end of the interview section. He explained that effective cyber power "has to be built on a strong CNI, resilience, good innovation, strong sort of pedigree, when it comes to cyber diplomacy, [and a] strong nexus between the private sector, government and academic and NGOs” (INTERVIEWEE A, 2020). This perception was later displayed in the 2022 NCSS as the "whole of a society approach" and the need to put cyber power at the core of foreign policy, developing equally offensive and defensive capabilities.

3.3 PARTIAL CONCLUSIONS

The chapter showed that the UK varied its cybersecurity approaches, going from a predominantly market approach (2009 – 2015) to a government approach (2016 – 2021) and a global one since its last NCSS. This variation led to different threats perception and self-perceptions, configuring an evolution of the state's digital mentality grounded deeply in economic and leadership aspects. In this regard, the UK's digital mentality led the country to assume a more assertive role toward cyberspace, culminating in its perception of cyber power. Interestingly, the chapter also reveals that despite using the term cyber power, the UK carefully wraps the concept with strong adjectives: "democratic" and "responsible."

4 FRANCE: DIGITAL MENTALITY AND CYBER POWER PERCEPTION

The present chapter presents France's digital mentality evolution, tracking France's threat perception and self-perception change over time. Besides, the chapter examines the state's perceptions of power and cyberspace over time. Thus, the chapter is divided into three subsections: general context and the phases of France's digital mentality, interviews inputs on cyber power perceptions, and partial conclusions.

4.1 FRANCE'S DIGITAL MENTALITY

France was one of the earliest countries to develop an overall policy toward information security. In 1986 it adopted a series of text regulations, establishing an inter-ministerial commission and delegation for the security of information services and a central service (ROMANI, 2008). Besides, with the Information Technology and Liberty Act (1978)[40] and the Godfrain Act (1988),[41] it became one of the first European countries to draft specific provisions for cybercrime and data protection (ENISA, 2010).

The 1994 Defense White Paper *(Le Livre Blanc sur la Défense*) emerged as the first document relating information technology as a threat to national security. The document highlighted that industrial and technological developments were bringing new concerns. Thus threats would be present in computer systems, such as "intrusion as well as on our energy production facilities or all communication networks" (LE LIVRE BLANC SUR LA DÉFENSE, 1994, p. 18, own translation)[42]. In this sense, it also recognized the role of information systems in the economy and that "Technologies have become, for their part, major issues of power" (LE LIVRE BLANC SUR LA DÉFENSE, 1994, p. 29, own translation). Therefore, responses to specific sectors would need to be sought and implemented jointly with European partners (whenever possible) to reduce economic vulnerabilities. One of the "privileged" sectors pointed out was the dual technology and industry, which would encompass information technology *(l'informatique*) (LE LIVRE BLANC SUR LA DÉFENSE, 1994) and thus the cyber realm.

[40] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

[41] "The Godfrain Act updated the French penal code by introducing a section regarding the intrusion in information systems (articles 323-1 to 323-7). This section has been updated several times since its introduction" (ENISA, 2010, p. 8).

[42] From the original in French: "intrusion comme sur nos installations de production d'énergie ou l'ensemble des réseaux de communication" (LE LIVRE BLANC SUR LA DÉFENSE, 1994, p. 18).

In this regard, France started building structures to protect its digital environment better. In 1996 France attributed to the General Secretariat for National Defense (SGDSN) a specific responsibility for identifying and monitoring risks affecting the security of information systems. In 2000 a national Computer Emergency Response Team called CERTA.[43] was created. A year later, the Central Directorate for the Security of Information Services (DCSSI), under the SGDSN, was set to assess and verify the security of public service networks and information systems, provide support to all administrations with inspection and advice, approve all encryption materials that protect classified data and prepare and implement the information systems security measures provided for by the Vigipirate[44] and Piranet[45] plans (ROMANI, 2008, p. 21). Besides the structures, in March 2004, a three-year plan to strengthen the security of State information systems was launched (ROMANI, 2008, p. 5).

Despite these arrangements, the French cyber security institutional framework remained dispersed. To call attention to the situation and the threat landscape of information technologies, Senator Pierre Lasbordes (2006) developed a parliamentary report on the matter that would inspire further developments regarding France's digital mentality. The Lasbordes report acknowledged that information systems, boosted by the Internet, changed the life of societies, including economically. Information Systems Security (ISS) would thus be a nationwide challenge, but for the state, it would mean a question of national sovereignty (LASBORDES, 2006, p. 9). In this regard, the report further linked information security to economic security.

The report said, "to be effective, a proactive economic intelligence policy must rely on reliable state and business information systems." Thus, it would be the companies' and the state's responsibility to invest in and accelerate the development of ICTs (LASBORDES, 2006, p. 45, own translation)[46]. The report is one of the first official documents to recognize the digital economy's importance relating to cybersecurity. However, it does so not as a dual

[43] Since 21 January 2014, "CERTA" has changed its name to "CERT-FR ."(CERT.FR, 2022).

[44] The Vigipirate plan is a central tool of the French system against terrorism. It associates all the stakeholders – the State, the local authorities, the public and private operators, as well as the citizens – with an attitude of vigilance, prevention, and protection (ANSSI, 2022a).

[45] Piranet is a government plan from the "Pirate" family of response plans. "The Pirate plans, complementary to the Vigipirate plan, are intervention plans triggered by the Prime Minister in the context of threats or attacks using specific means of aggression or affecting particular environments." In this sense, "Piranet is devoted to state intervention in the event of a major IT crisis" (ANSSI, 2022a).

[46] From the original in French: « Pour être efficace, une politique volontariste d'intelligence économique doit notamment s'appuyer sur des systèmes d'information fiables de l'État et des entreprises" (LASBORDES, 2006, p. 45).

engine like the UK but as a means to independent action, a more significant power aspect for France.

The report also pointed to the emerging threat landscape of information systems. A list of cyber attackers' profiles was further developed as an annex to the report. Cyber attackers were divided into script kiddies, hacktivists, and hackers. Interestingly, the last one followed a technical division between white, gray, and black hats. The black hat was the most dangerous, including virus creators, cyber spies, cyber terrorists, and cybercriminals (LASBORDES, 2006, p. 161-162).

Moreover, the report listed four types of attack motivations (that could overlap): ludic, greedy, terrorist, or strategic. In this sense, it calls attention that a particular concern with espionage and disinformation emerges regarding strategic motivation. Specifically, the document said that either states, organized groups, or companies could “effectively use any weaknesses in information systems to gain knowledge of sensitive or confidential information." It continued by stating: "Disinformation and destabilization are very powerful and easy to implement means with a multiplicative effect due to our dependence on information" (LASBORDES, 2006, p. 29, own translation)[47].

The report also identified as targets of these attacks: critical national infrastructures, the State, companies, academic entities, universities, research centers, engineering schools, and citizens (LASBORDES, 2006). In fact, with a very technical focus, it pragmatically even mentioned aspects such as social engineering and individual manipulation as part of the threat landscape (LASBORDES, 2006, p. 40).

Besides issues regarding sovereignty and the threat landscape, it calls attention that the report reinforced that France should act efficiently and reactively to the challenges of the digital environment. In this regard, Lasbordes (2006) pointed to a lack of cohesion. This was due to an overall dispersion "of resources, skills, and policies" (LASBORDES, 2006, p. 50). The report also compared the developments of other countries in the subject, among them the United Kingdom, Germany, and the United States, pointing out that France was lagging on ISS. It thus provided six main axes of recommendations to the French government, among them the need to ensure the security of vital infrastructure and the strengthening of technology and product development policy (LASBORDES, 2006).

[47] From the original in French: “un État, des groupes organisés ou des entreprises, peuvent utiliser avec efficacité les faiblesses éventuelles des systèmes d’information afin de prendre connaissance d’informations sensibles ou confidentielles (…) La désinformation et la déstabilisation sont des moyens très puissants et faciles à mettre en oeuvre avec un effet multiplicatif dû à notre dépendance vis-à-vis de l’informatiobn. (LASBORDES, 2006, p. 29).

The recommendations and awareness that the Lasbordes report brought to French decision-makers served as a base for further reasoning displayed in the 2008 White Paper on Defense and Security. This new reasoning would seek to implement a greater cohesion institutionally and encompass the impact of new cyber events, such as the Estonia cyberattacks in 2007. Besides, a new parliamentary report was produced on the subject.

4.1.1 The first phase (2008-2013): Techno-military approach

The 2008 French White Paper on Defense and Security reinforced the idea of ICTs playing a transformative role in society. Defining cyberspace as "the meshing of the whole networks" (DÉFENSE ET SÉCURITÉ NATIONALE, 2008, p. 53, own translation)[48], the White Paper explained that threats would have many forms. These include malicious blocking, physical destruction, neutralization of computer systems, data theft or distortion, and control of a system for hostile purposes (DÉFENSE ET SÉCURITÉ NATIONALE, 2008). In this regard, one can once again perceive a technical approach to the subject.

Within this approach, the 2008 White Paper highlighted that states were already mapping offensive cyber strategies, indicating that passive defense was not enough anymore, despite being necessary still. In this scenario, the White paper showed the need for governmental lead and a mentality change toward an active in-depth defense, which would require "intrinsic systems protection with permanent surveillance, rapid response and offensive action" (DÉFENSE ET SÉCURITÉ NATIONALE, 2008, p. 53, own translation)[49]. By calling the military concept of defense in depth[50]. One can infer that a robust military component would make part of France's perception of cyberspace and, thus, its digital mentality. This would consolidate what Desforges (2018) called a techno-military approach.

The White Paper, in this context, also exposed the idea of national offensive cyber capabilities development (Lutte Informatique Offensive) for the first time, emphasizing the need for matching these developments with domestic legal principles and proportionate responses. Besides, it cites the term "cyber-war" several times but does not develop it further.

[48] From the original in French: "(…) constitué par le maillage de l'ensemble des réseaux (…)" (DÉFENSE ET SÉCURITÉ NATIONALE, 2008, p. 53).

[49] From the original in French: "(...) combinant protection intrinsèque des systèmes, surveillance permanente, réaction rapide et action offensive (…)" (DÉFENSE ET SÉCURITÉ NATIONALE, 2008, p. 53).

[50] This concept "deals with the slowdown of the progression of an attack by using different successive layers, such as fortifications, troops, and field works, instead of concentrating all resources onto a single defensive line" (CHERICI *et al.*, 2016, p. 36).

It also emphasizes France’s need to maintain strategic and political autonomy in some key areas, including cybersecurity (DÉFENSE ET SÉCURITÉ NATIONALE, 2008).

The concern over strategic autonomy is relevant here as it dates back to postwar French military strategy. According to Desforges (2018), this concept focuses on the development of a state’s own operational and industrial capacities, and despite advocating for self-reliance, it does not exclude cooperation. Laudrain (2019a) explains, "it is characterised by a strong sense of national independence but recognises the need for a powerful political Europe." Thus, the European element is present in themes such as cybersecurity and cyberdefense and the recognition of improving the defense industrial base favoring technologies in the cyber realm.

A final remark on the 2008 White Paper was its emphasis on pushing a cohesive state action indicating the need for the creation of a new agency responsible for information systems security (*Agence de la sécurité des systèmes d'information*) (DÉFENSE ET SÉCURITÉ NATIONALE, 2008). This Agency was further developed in 2009, resulting in the French National Cybersecurity Agency (ANSSI).

In this regard, ANSSI and MoD would make the two pillars of a centralized institutional model to deal with cyberspace. These entities would each carry different yet complementary capacities: defensive and offensive. This separation would mark the French vision of cyberspace and its further digital mentality development. In this regard, ANSSI would be in charge of cybersecurity in general (including risk management) and MoD to protect networks underpinning its action and integrate digital elements into military operations (DARWISH; ROMANIUK, 2021). Notwithstanding this division, an early concern on the efficiency of ANSSI would be put in place with a parliamentary report delivered in 2008, after the launch of the White Paper: Roger Romani's report.

The 2008 report aimed to further developed notions of cyber defense, thus interested in the "attacks on information systems likely to jeopardize the security and defense of the country and the means of protecting against them" (ROMANI, 2008, p. 6, own translation)[51]. It exposed that cyber attacks were a concrete reality, citing the Estonia 2007 cyber-attacks and the espionage attacks suffered by France in 2007. The report also unveiled an early self-

[51] From the original in French: “Il s’intéresse essentiellement aux atteintes portées aux systèmes d’information susceptibles de mettre en cause la sécurité et la défense du pays et aux moyens de s’en protéger” (ROMANI, 2008, p. 6).

perception of France being insufficiently prepared and organized "in the face of the threat of computer attacks" (ROMANI, 2008, p. 6, own translation)[52].

The 2008 report identified some main threats to government and business systems within the threat landscape. These threats were Denial of Services (DoS) and intrusion to misappropriate information. In this sense, it is interesting that the report differentiates cybercriminal activity from cyber attacks regarding national security by using the terminology "computer war" (*Guerre Informatique*). The "computer war" would "characterize actions aimed at paralyzing the systems of an institution or a company, or at diverting or distorting its data" (ROMANI, 2008, p. 11, own translation)[53]. In this regard, the report highlighted three forms of computer warfare:

> - The war against information, which attacks the integrity of computer systems to disrupt or interrupt their operation;
> - The war for information that aims to penetrate the networks in order to recover the information which circulates there or is stored there;
> - Information warfare, which uses the computer vector for the purpose of propaganda, disinformation, or political action. (ROMANI, 2008, p. 12, own translation)[54]

The report also pointed to different types of cyber attackers. These included: hackers (including patriotic hackers), terrorists (using the Internet for propaganda and proselytism, as well as a means of communication), and states (regarding mainly cyber espionage). It thus emphasized that the two major concerns regarding cybersecurity involved the protection of services essential to the functioning of the country or its defense and the protection of sensitive information from a political, military, or economic point of view (ROMANI, 2008). Considering these elements, the report recalled the institutional framework of France on cybersecurity, mentioning the ideas of the 2008 White Paper on Defense and Security.

In this regard, the report further explains the difference between a passive and active defense. The first would be "defined as a simple recourse to automatic network protection systems (firewalls, antivirus), placed at the border between them and the outside." While the

[52] From the original in french: "face à la menace d'attaques informatiques" (ROMANI, 2008, p .6).

[53] From the original in French: "**guerre informatique** pour caractériser les actions visant à paralyser les systèmes d'une institution ou d'une entreprise, ou à en détourner ou déformer les données." (ROMANI, 2008, p. 11).

[54] From the original in French:

- "la guerre contre l'information, qui s'attaque à l'intégrité de systèmes informatiques pour en perturber ou en interrompre le fonctionnement
- la guerre pour l'information, qui vise à pénétrer les réseaux en vue de récupérer les informations qui y circulent ou y sont stockées
- la guerre par l'information, qui utilise le vecteur informatique dans un but de propagande, de désinformation ou d'action politique" (ROMANI, 2008, p. 12).

second would mean "a real ability to monitor "borders" and to constantly adapt to a threat that evolves daily, with new vulnerabilities constantly appearing" (ROMANI, 2008, p. 43, own translation)[55]. Therefore, to have an active defense, the report indicated the need to set up a detection center responsible for permanently monitoring sensitive networks to create an early detection capacity and the development of offensive capabilities. The document put three reasons for the development of offensive capabilities: technical (concerning better defense), strategic (for deterrence), and the fact that "cyberspace seems inevitably destined to become a field of struggle" (ROMANI, 2008, p. 45, own translation)[56].

In this sense, the report exposed a self-perception of France still lagging in the topic. Thus, the report recommended broadly that the country: leveraged national resources up to the level of other European countries, give more force to the information systems security policy (providing clear coordination among the key actors involved), and strengthen the partnership with the economic sector (ROMANI, 2008).

The concerns raised by the White paper and the Romani report reinforce the idea of bridging structural gaps in France's cybersecurity. ANSSI, in this sense, was conceived as a civilian organization that reports to the General Secretary for Defence and National Security (SGDSN), which in turn, assists the Prime Minister in his responsibilities related to national defense and security. The Agency thus "focuses primarily on the social, economic, and governmental aspects of cyber issues" (BAEZNER, 2018, p.10).

To generate the cohesion element pointed out by the Romani Report, in 2010, the President decided to make the Agency responsible for the defense of information systems and its security role (ANSSI, 2011). Thus, ANSSI possesses a department titled Operational Center for the Security of Information Systems (COSSI), which collaborates closely with the Analysis Centre for Defensive Cyber Operations (CALID), its counterpart in MoD (BAEZNER, 2018).

Also, in 2010 the Parliamentary Intelligence Delegation (DPR), in its annual report, exposed it had regular contact with the departments responsible for coordinating national security and intelligence matters. Among its interlocutors were the services which depend on these bodies, such as ANSSI (WARSMANN; ROHAN, 2010).

[55] From the original in French : “une véritable capacité de surveillance des « frontières » et l’aptitude à s’adapter en permanence à une menace qui évolue de manière quotidienne, de nouvelles vulnérabilités apparaissant em permanence” (ROMANI, 2008, p. 43).

[56] From the original in French: “e cyberespace paraît inévitablement voué à devenir un domaine de lutte” (ROMANI, 2008, p. 45).

ANSSI launched the first French National Cyber Security Strategy in 2011. The National Cyber Security Strategy (NCSS) defined cyberspace as "The communication space created by the worldwide interconnection of automated digital data processing equipment." At the same time, the cyber defense was understood as "The set of all technical and non-technical measures allowing a State to defend in cyberspace information systems that it considers to be critical" (ANSSI, 2011, p. 21). These broad definitions would allow an edge for displaying offensive and defensive cyber operations in the digital world.

In this sense, and building on the 2008 White Paper observations, the NCSS set four strategic objectives:

a) Become a world power in cyber defense.

b) Safeguard France's ability to make decisions by protecting information related to its sovereignty.

c) Strengthen the cybersecurity of critical national infrastructures.

d) Ensure security in cyberspace.

By putting as a first strategic objective to be a world power in cyber defense, one can infer that the country recognized power relations occurring within cyberspace, particularly considering these relations to be around "power to control." Besides, this first indicate France's changing its self-perception from a "lagging behind" position to a "catching up" one. In this sense, France's self-perception was of an emerging power in cyber defense.

Moreover, one can recall the idea of strategic autonomy by calling for its sovereign retention. In this sense, the NCSS explained that for France to maintain its independence, it must "master cryptographic techniques and key technologies needed to design our security products" (ANSSI, 2011, p. 12). The Crypto AG case is an example that can explain this reasoning[57]. This element is evidence of the concerns over data and the relevance of intelligence for the country.

Besides the concerns over data, other elements of strategic autonomy appear in the NCSS, especially in the seven areas of action discriminated by the NCSS:

a) Anticipate and analyze.

[57] The Crypto AG case refers to the disclosure of Rubic Operation, involving the American Central Intelligence Agency (CIA) in partnership with the German intelligence agency Bundesnachrichtendienst (BND). Both agencies secretly purchased the Swiss coding machine manufacturer, Crypto AG, in 1970, manipulating products from its design and allowing both countries to have access to classified information from a large portfolio of countries. Despite Germany withdrawing in the 1990s, the USA continued the Operation until 2018, causing major impact with the disclosure of this surveillance (DOBSON; DYMYDIUK; MAINWARING, 2020; MILLER, 2020).

b) Detect, alert and respond.

c) Enhance and perpetuate our scientific, technical, industrial, and human capabilities.

d) Protect the information systems of the state and the operators of critical infrastructures.

e) Adapt French Legislation.

f) Develop our international collaborations.

g) Communicate, inform and convince.

We can emphasize actions 4 and 6 as strategic autonomy elements. In other words, it represents the development of industrial capabilities and acknowledges the importance of leveraging an international network with partners, including the European Union.

The actions further demonstrate that France mirrored some conventional ideas of power into the cyber realm, such as diplomatic (action 6), military (action 2), economic (action 3), and political (action 7) powers. It also is interesting to point out an element of "horizon scanning" present in the development of action three regarding human resources, and thus the inclusion of monitoring emerging technologies.

Despite not explicitly, the NCSS also exposed France's understanding of a threat landscape, including illicit activities carried directly or indirectly by foreign States, terrorist activities online, and cybercrime. The NCSS emphasized the two first as threats to national security. It explains, "In the near future, foreign States or terrorist groups could attack the critical infrastructures of States that they consider as ideologically hostile." The potential for attacks on critical infrastructure is thus used to justify France to develop its "cyberdefence capability" (ANSSI, 2011, p. 11).

The year 2011 would also mark other developments in cyber defense. The Ministry of Defense and the armed forces adopted a joint cyberdefense concept. A year later, a cyber defense doctrine was developed (BOCKEL, 2012, p. 82), but it was not publicly disclosed at the time. Besides, a cohesive element was set. The DPR exposed to have "examined the various aspects of our cybersecurity strategy, in particular concerning the organization and coordination of the various players and the development of the means devoted to this strategy" (CARRÈRE, 2012, p. 12, own translation)[58].

[58] From the original in Fench: "Elle [DPR] a aussi examiné les différents volets de notre stratégie en matière de cybersécurité, en ce qui concerne en particulier l'organisation et la coordination des différents acteurs et l'évolution des moyens consacrés à cette stratégie" (CARRÈRE, 2012, p. 12).

In 2012 a new parliamentary report on the topic of cyberdefense also emerged. The Bockel report said that despite France catching up with other nations on the subject, its domestic mechanisms presented remaining gaps (BOCKEL, 2012, p. 68). In this sense, it highlighted: the attacks against the information systems of the Ministry of Economy and Finance (discovered at the end of 2010, on the eve of the French presidency of the G8 and the G20)[59] and the cyberespionage of the Areva group[60]. Moreover, the revelations that the Presidency of the Republic[61] would have been the subject of one or more large-scale cyber attacks were also displayed in the report (BOCKLE, 2012).

The Bockle report maintained a technical approach to the subject, explaining the operational mechanisms for malware detection and forms. However, it is worth noticing that the threat landscape assessed changed. The report differentiated cybercrime activities from cyber defense, employing computer war terminology. However, the attacks included sabotage, destruction, espionage, and destabilization. This can be attributed to the malware Stuxnet's international impact, which was cited as an illustrative case.

The report also mentioned some perils from hackers (including patriotic hackers and hacktivism), cyber criminals, cyber terrorists, and states. In this regard, it calls attention that the report explained that cybercrime, as a potential destabilization element of the national economy, would "justify resolute action on the part of the public power to strengthen the means of combating this scourge" (BOCKLE, 2012, p. 35, own translation)[62]. The report also emphasized that terrorists used the Internet for propaganda and proselytizing purposes and as a means of communication. However, it indicated that no major terrorist attack by computer had happened (BOCKLE, 2012, p. 35). On mentioning state action, the report showed the feasibility of cyber war as extreme, arguing that cyberspace would not necessarily imply an "autonomous medium of war" nor would it dominate the other conventional domains of war. Still, the rapporteur affirmed the feasibility of using information systems attacks as supportive of military campaigns, given the example of the Georgia conflict in 2008 (BOCKEL, 2012, p. 36, own translation)[63]

After the assessment, the report highlighted some recommendations, among them one related to making “cyber defense and the protection of information systems a national priority,

[59] Considered "the first attack against the French State of this magnitude and on this scale" by the Director-General of ANSSI, Mr. Patrick Pailloux (BOCKLE, 2012, p. 21, own translation)

[60] Areva SA is a French multinational group specializing in nuclear power (AREVA, 2022).

[61] One example was the disclosure by Wikileaks of the US spying on Elysée, during the Sarkozi-Holland handover (SPARK; MULLEN, 2015).

[62] From the original in French: “justifient donc une action résolue de la part de la puissance publique pour renforcer les moyens de lutte contre ce fléau” (BOCKLE, 2012, p. 35).

[63] From the original in French: “milieu autonome de la guerre” (BOCKLE, 2012, p. 36).

taken to the highest level of the state, particularly in the context of the new White Paper and the future military programming law," and the other to "Reinforce the staff, resources, and prerogatives of the National Information Systems Security Agency" (BOCKLE, 2012, p. 5, own translation)[64].

The Bockle report shows us that France was still looking for its structural and domestic development, despite its commitment to a broader action space. In this regard, the 2012 DPR's annual report brought a section devoted to cyber for the first time. The DPR's report stressed a concern with "the constant progression of the "cyber" threat, which materialized several times in 2012 in the form of computer attacks against French administrations and companies" (SUEUR; ADAM, 2013, p. 7, own translation). In this sense, the DPR's report made some recommendations on the issue of "cyber," among them the need to prioritize the topic for France's national defense and security and the need to develop offensive capabilities. Regarding this last point, the document stated: "It seems difficult, in fact, to conceive of a defensive policy without knowing the methods and means of attack." (SUEUR; ADAM, 2013, p. 18, own translation)[65].

In the context of these discussions, in 2013, a new White Paper on Defense and Security was launched, finally establishing the priority of cyber defense for France. The document assessed a threat landscape to national security comprised of cyber espionage and cyber attacks against critical infrastructure, arguing that cybercrimes would remain at a lower level of threats, aside from national security concerns. According to the White Paper

> [...] national security is threatened by attempts to infiltrate digital networks for purposes of espionage, regardless of whether they target State IT systems or those of companies. An attack designed to destroy or take remote control of computer systems used to manage essential infrastructure, automated control systems of potentially dangerous industrial systems, not to speak of weapons systems or strategic military capabilities, might have very serious consequences (MINISTÈRE DE LA DÈFENSE, 2013, p. 43).

The White Paper explained that defensive and intelligence capabilities would be developed considering these threats.

Moreover, it stated Frances's perception of what type of cyber attack could be considered an act of war. According to the document, the recurrence of information systems

[64] From the original in French: "Priorité nº 1: Faire de la c**yberdéfense et de la protection des systèmes d'information une priorité nationale**, portée **au plus haut niveau de l'Etat**, notamment dans le contexte du nouveau Livre blanc et de la future loi de programmation militaire.(…) Priorité nº 2: Renforcer l**es effectifs, les moyens et les prérogatives de l'Agence nationale de sécurité des systèmes d'information" (**BOCKLE, 2012, p. 5).

[65] From the original in French: "Il paraît difficile, en effet, de concevoir une politique défensive sans connaître les méthodes et les moyens d'attaque" (SUEUR; ADAM, 2013, p.18).

infiltration “notably on the part of states” could suggest a methodical information collection aiming to facilitate "a large-scale attack in a conflict situation." In this sense, if it could "paralyse whole swathes of a country's activity, trigger technological or ecological disasters and claim numerous victims," it could be considered an act of war (MINISTÉRE DE LA DÈFENSE, 2013, p. 48). By exposing this view, the White Paper set France's comprehension of a cyber attack as equivalent to force demonstration, in a way justifying further the necessity of defensive capabilities development and coercive engagements, in another reinforcing the mirroring of the physical ideas into the digital world.

The White Paper also recalled the idea of strategic autonomy in cyberspace. It exposed that the "capacity to detect and protect ourselves against cyber attacks and to identify those responsible for them has become an element of national sovereignty" (MINISTÈRE DE LA DÈFENSE, 2013, p. 100). Thus, France would need to have the capacity to autonomously produce security systems, mainly regarding cryptography and attack detention. In this context, the document also explained the importance of Europe to “have the capacity to protect its vital infrastructure and its industrial, scientific and technical potential against attacks or cyberattacks conducted by States or organisations motivated by espionage or sabotage” (MINISTÈRE DE LA DÈFENSE, 2013, p. 52). Thus, contributing to creating a stable environment within the European Union and, hence, the French strategic surroundings.

Besides, the 2013 White Paper exposed that the response policy to major "IT attacks" would be based on the principle of a "global approach," complemented by two aspects:

> - the implementation of a robust and resilient posture to protect state information systems, operators of essential infrastructure, and strategic industries, paired with an operational organisation to defend these systems, coordinated by the office of the Prime Minister and supported by close cooperation of the different state agencies, to identify and qualify as early as possible any threats to which our country is exposed;
> - a capacity for a global and appropriate governmental approach to attacks of varied nature and magnitude, relying initially on all diplomatic, judicial, or police resources, but without ruling out progressive use of Ministry of Defence resources in the event that national strategic interests are threatened (MINISTÉRE DE LA DÈFENSE, 2013, p. 102).

In this regard, a solid defensive posture is reinforced, along with the concern of using proportional responses. Besides, the idea of a global approach toward cyberspace had started to be set in motion.

The global approach would be sedimented partially due to the Snowden revelations in 2013. the revelations demonstrated that France was under USA surveillance and generated a significant domestic impact. One can infer an impact of the French push as the principal negotiator, in 2013, for the adoption of the Wassenaar Arrangement[66] of the “intrusion software” and “[Internet Protocol] network communications surveillance systems to the list of dual-use technologies (DARWISH; ROMANIUK, 2021, p. 69). Another impact was the dialogue between the French President of the Republic, at the highest level, with allies (including then the USA) to establish a "code of good conduct" in the area of personal data interception (SUEUR, 2014, p. 10, own translation)[67].

The French media also raised suspicions over the national intelligence services. For example, "LeMonde" wrote a series of articles affirming that the General Directorate for External Security (DGSE) maintained with French operators the same relationship as the National Security Agency (NSA) with operators operating on USA territory. The DPR addressed the accusations refuting them and reinforcing that no legislative framework would authorize the collection and that “Consequently, no company is obliged to respond to any requests, and none of them has any interest in doing so.” (RAFFARIN; URVOAS, 2014, p.139). In this regard, the 2014 DPR's annual report explained the placed control on intelligence services, mentioning the relevance of the Military Planning Law *(Loi de Programmation Militaire* -LPM).

The LPM was enacted in 2013 but designed for 2014-2019. It established a link between conventional military operations and cyberdefense and provided control of the government's activity in the field of intelligence. The annexed report disclosed in the *Journal Officiel Lois et Décrets* n° 294 (REPUBLIQUE FRANÇAISE, 2013) explained that one of the priorities of the LPM 2014-2019 would be the focus on increasing France’s cyberdefense power. In this regard, the 2014-2019 LPM granted an overall investment of €1 billion to cyber defense intended to be divided between the capacity needs of the ministry (human resources, technical means) and the research and innovation sector (JOUBERT, 2014).

According to Desforges (2018), the Snowden revelations and the evident dependencies of USA digital platforms attached to the Daesh online propaganda contributed to France's strategic thinking thematic broadening. Besides, institutional actors in the background, especially the Ministry of the Interior and the Ministry of Foreign and European Affairs, gained more prominence. In this sense, Desforges argues that a double opening on France's strategic thinking happened: on actors and subjects. Building on this argument, a new threat

[66] The Wassenaar Arrangement was established in 1996 and constitutes a voluntary export control regime whose members exchange information on transfers of conventional weapons and dual-use goods and technologies (ARMS CONTROL ASSOCIATION, 2022).

[67] From the original in Feench: “ « code de bonne conduite»” (SUEUR, 2014, p.10).

landscape and self-perception was developed. Thus, the second phase of France's digital mentality can be explored.

4.1.2 The second phase (2014-2021): Global approach

To strengthen its strategic autonomy France published in 2014 Cyberdefense Pact (*Pacte Défense Cyber*), whit six axes and 50 measures. The six axes were:

a) Tighten the level of security of information systems and the means of defense and intervention of the ministry and its major, trusted partners;

b) Preparing for the future by stepping up the research effort, both technical and academic, and operational, while supporting the industrial base;

c) Strengthen the human resources dedicated to cyber defense and build the associated career paths;

d) Develop the Center of Excellence in cyber defense in Bretagne for the benefit of the Ministry of Defense and the national cyber defense community;

Cultivate a network of foreign partners, both in Europe and within the Atlantic Alliance and in areas of strategic interest; and Promote the emergence of a national cyber defense community by relying on a circle of partners and reserve networks (MINISTÉRE DE LA DÈFENSE, 2014).

Among the measures, it calls attention the creation of a citizen reserve (*Le Réseau cyberdéfense de la réserve citoyenne* – RCC) to provide a network of committed cyber experts, engaging thus civilians in support of the military. Besides, the launch of the Center of Excellence by the MoD happened in February 2014, co-located with the Directorate General for Armaments, "which itself institutes important cyber efforts, and integrates the MOD's cyber skills in terms of training, research, and technology" (VITEL; BLIDAL, 2015).

Other initiatives were put in place for France's strategic autonomy. Like the roadmap of the Cybersecurity plan (Plan 33) for a New Industrial France, which the 'ANSSI supported, and the system subsidizing dual innovation projects, funding called RAPID (*Régime d'Appui à l'Innovation Duale*) announced by the MoD (CYBER CERCLE, 2015). Moreover, a concrete action toward the global approach mind setting was also the creation, in October 2014, of the position of a Cybersecurity Coordinator within the Ministry of Foreign Affairs (VITEL; BLIDAL, 2015), and the launched National Intelligence Strategy, which identified cyberattacks as a significant national threat (BAS, 2018).

Notwithstanding these efforts, major cyber attacks in 2015 would impact France's digital mentality. In January 2015, a wave of cyberattacks on private and State websites was deployed along with terrorist attacks that started with the attack against the Charlie Hebdo magazine. Radical extremist hackers claimed more than 1,500 attacks in this period and ANSSI thus activated its crisis system. Further, on 8 April, terrorist attacks against TV5 Monde television news channel were deployed. The Twitter accounts and the Facebook page of the international channel were appropriated by the Cybercaliphade of a terrorist group called Daesh. The cyber attack was considered a sabotage act by ANSSI.[68] It resulted in the disfigurement of the channel's website, the cease of its broadcast, and the dissemination of messages on social networks claiming to come from TV5 Monde but supporting Daesh. In this context, the intervention of ANSSI (in collaboration with the teams of the channel) only ended a few months later, in July (ANSSI, 2016; VITEL; BLIDAL, 2015).

The impact of these cyber attacks generated further discussions in France, and a new National Cyber Security Strategy was launched in 2015.

The 2015 National Cyber Security Strategy set five strategic objectives for France,

a) Fundamental interests, defense, and security of state information systems and critical infrastructures, major cybersecurity crisis
b) Digital trust, privacy, personal data, “cybermalevolence.”
c) Awareness raising, initial training, continuing education
d) Environment of digital technology businesses, industrial policy, export, and internationalization
e) Europe, digital strategic autonomy, cyberspace stability. (PREMIER MINISTRE, 2015).

These objectives were built upon a new threat landscape, encompassing states, terrorists, criminals, and digital platforms monopolies. The strategy explains that "Digital platforms, including social networks, can shape opinion more insidiously and are often vectors of values that are not those of the French Republic” (PREMIER MINISTRE, 2015, p. 20). Therefore, the opinions against France's interests would be considered "an attack on defence and national security which is sanctioned by law” (PREMIER MINISTRE, 2015, p. 20).

[68] Investigators suspected that a threat actor associated with the Russian military intelligence services, APT28, was involved. Its involvement was further “corroborated by cybersecurity companies such as Trend Micro and the former chief of the investigation of ANSSI” (DESFORGES; GÉRY, 2021).

Moreover, the 2015 NCSS openly recognized cyber espionage among States (including between allies) as a fact of countries' political increased mistrust and that cyberspace had become "a place of conflict and often unfair competition"(PREMIER MINISTRE, 2015, p. 38). This perception reflects a Hobbesian view of cyberspace in which "anticipation and prevention" would be essential tools. The NCSS explained that for 2020 these two tools would be the priority for the competent information systems security authorities. Besides, their use would entail "ensuring that the digital products and services or those that involve digital technology, which are designed, developed and produced in France, are among the safest in the world" (PREMIER MINISTRE, 2015, p. 33).

The recall for promoting France's industrial capabilities was thus a reference to the strategic autonomy thinking in the collective imaginary of the country. On this subject, the NCSS linked the industrial cybersecurity development of Europe to France, recognizing its importance for the national interest. According to the NCSS:

> The answer to this issue of sovereignty requires first and foremost the maintenance of a strong and competitive national and European industry in the specialised field of cybersecurity products and services. In general, it requires the development, in France and Europe, of a digital equipment and service offer that provides clients with the guarantees of security and trust adapted to the issues and use (PREMIER MINISTRE, 2015, p. 30).

In this regard, France put Europe as a preferred political platform to leverage cybersecurity. Placing itself as the "driving force behind European strategic autonomy" (PREMIERE MINISTRE, 2015, p. 39), the country exposed its international strategy of multilateral and bilateral engagement and the promotion of cyber capacity building. Besides, a new law enacted on 30 November 2015[69] established a legislative mechanism to regulate the surveillance of international communication that "transit through France" (ADAM; BAS, 2017, p. 71, own translation).[70]

In this context, not only the enlargement of the perceived threat landscape was set but also a change in France's self-perception in the digital domain. The document briefly mentioned the idea of France being a "Digital Republic." Moreover, in a 2015 interview, the Minister of Defense Jean-Yves Le Drian exposed the improvements that the LPM 2014-2019 brought to France's cybersecurity, saying that "In the entourage of the minister, it is estimated

[69] LOI n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales.

[70] From the priginal in French: " transitent par la France" (ADAM; BAS, 2017, p.71).

that France is one of the very best nations in the world, behind the three great powers (the United States, China, and Russia)" (CABIROL, 2015, own translation)[71]

If one can infer that France perceived itself as a relevant cybersecurity/cyber defense power, the meaning of “Digital Republic” (*République Numérique*) was further discussed within French society, being later transposed to a national Law in 2016. In this regard, Law n° 2016-1321 of 7 October 2016 was developed to regulate the new aspects of the digital economy and was built around three axes:

a) The circulation of data and knowledge.

b) The protection of individuals in the digital society.

c) Universal access to digital technology.

This design shows the aim of France to transpose its offline values into the virtual world as a democracy. According to its Statement of Reasons, the objective of the French government was “to give France a head start in the digital field by promoting a policy of openness to data and knowledge” as well as “to strengthen their [individuals] power to act and their rights in the digital world.”(LÉGIFRANCE, 2022, own translation) Thus, the numerous provisions related to data protection in the Law represent several key amendments under the French Data Protection Act of 1978 and other laws before the GDPR entered into force in 2018 (PROUST, 2016).

In addition, it calls attention to the fact that the regulation of platforms was put at the center of the Law (GATEAU; FARON, 2016). Specifically, the Law requires public communication service providers to offer users functionality for recovering data associated with their accounts through portability and data recovery. Moreover, it demands transparency and competition "via the loyalty of platforms and information intended for consumers, particularly with regard to online reviews, methods of referencing, classification and dereferencing as well as general conditions of use" (STRATÉGIE INTERNATIONALE DE LA FRANCE POUR LE NUMÉRIQUE, 2017, p. 19). Therefore, a paradox emerged in France’s cyber policy. Desforges (2018, p.171) explained it by saying that despite France's inclusive approach toward actors, one can observe a policy practice of s "parent-state" (*État-parent*), setting the rules for all private actors.

France's aim to protect its cyber capacity internationally was reflected by the Defense Minister, Mr. Jean-Yves Le Drian, who publicly mentioned the development of French

[71] From the original: “Dans l'entourage du ministre, on estime que la France fait partie des toutes meilleures nations au monde, derrière les trois grandes puissances (États-Unis, Chine et Russie)”.

offensive capabilities. In a speech, he said a command within the armed forces would be created (CYBERCOM) to plan, control, and conduct cyber defense operations. This command would have what he called "digital action" among its pillars, covering various missions such as offensive actions or intelligence (VIE PUBLIQUE, 2016). In 2017 COMCYBER was established.

Besides, in May 2016, ANSSI's 2020 Strategy was launched, making the Agency a European reference in cybersecurity. ANSSI's strategy was planned to implement the NCSS operationally and sets the Agency's direction and fields of intervention. According to ANSSI's Director Guillaume Poupard, this strategy was intended to develop an approach that would bring together "all the skills of the agency," consolidating what was already undertaken, improving France's operational methods, and preparing for the future (ANSSI, 2017, p.11).

In this regard, France was displaying its reasoning in practice. The global approach reinforced the application of conventional powers (political, economic, diplomatic, military, and informational) toward cyberspace. Following a more consolidated digital mentality, France's more assertive posture emerged in 2017.

During the 2017 presidential elections, a major hack leaked internal emails and other documents related to the then-presidential candidate, Emanuel Macron (WILLSHER; HENLEY, 2017). Nevertheless, the Macron leaks were not the only major cyber event impacting France. The Wannacry and Notpetya ransomware attacks affected France as well. This scenario was reflected in the major cyber-attack tendencies that the 2017 ANSSI report listed: democratic process destabilization, economic destabilization, operational modes sophistication, indirect character, non-discriminatory character, and resurgence of destructive effects (ANSSI, 2018, p. 9).

In this sense, France launched the Defence and National Security Strategic Review, which stated its decision to adopt a permanent cybersecurity posture (REPUBLIQUE FRANÇAISE, 2017, p. 71). Besides, it reinforced the importance of France's retaining its capability of sovereign action in cyberspace, which would require "expertise in both industrial and regulatory aspects of the relevant technologies, equipment, services, and data acquisition, storage, and processing capabilities" (REPUBLIQUE FRANÇAISE, 2017, p. 64). The document also characterized cyber as an amplifier of military actions. It acknowledged that "disinformation efforts amplified by the Internet can lead to soft forms of subversion, intended to exacerbate tensions within the targeted society, as well as to influence and to foster political paralysis" (REPUBLIQUE FRANÇAISE, 2017, p. 47).

However, a proactive element calls further attention: attribution. The Defence and National Security Strategic Review explained that "the characterisation and attribution of attacks" at the core of France's need for autonomous assessments, placing thus the ability to detect and attribute, "based on gathering both human and technical intelligence," as key factors for France's development of cyber offensive and defensive capabilities (REPUBLIQUE FRANÇAISE, 2017, p. 72). It is important to highlight that France's posture toward attribution is more discrete than other States. Desforges and Géry comment, "Most consistently, France falls short of naming and shaming states for cyberattacks, " carefully drafting its statements not to accuse states. In this regard, Laudrain (2019a, p. 9) explains France prefers "red phones over megaphones," meaning a preference for direct dialogues with the culprits of the cyber attacks instead of naming and shaming them. Notwithstanding, as Desforges and Géry (2021) highlighted, some statements made by the French authorities, such as the ones on Turla (2019), Sandworm, and APT31 (these both in 2021) "designed an intrusion set," getting close to public attributions.

Besides the Strategic Review, another base document was launched on France's global posture on cyber issues: the international digital strategy. Based on three key pillars: governance, the economy, and security, it exposes France's objective to become more relevant internationally by helping to draw both a digital roadmap and framework for the cyber world. According to the document: "multilateral, realistic and pragmatic creativity is the method that France wishes to adopt in order to define the digital world that we want and the role that France and Europe must play in it in the decades to come." (STRATÉGIE INTERNATIONALE DE LA FRANCE POUR LE NUMÉRIQUE, 2017, p. 3, own translation)[72].

The International Digital Strategy also reinforced France's self-perception as a digital republic. According to the document:

> France intends, in this respect [to make France a Digital Republic], to promote its digital vision, whether in terms of the digital transformation of the State, the opening of public data or the protection of personal data, while by developing open ecosystems, from which French start-ups will be able to shine beyond our borders and in which entrepreneurs, talents and investors from all over the world will be welcomed. It is also about exploring and promoting all new forms of creation (transmedia, digital arts, new writing, etc.) and promoting French creation in the

[72] From the original in French: "Cette créativité multilatérale, réaliste et pragmatique, c'est la méthode que la France souhaite porter afin de définir le monde numérique que nous souhaitons et le rôle que la France et l'Europe doivent y jouer dans les décennies à venir" (TRATÉGIE INTERNATIONALE DE LA FRANCE POUR LE NUMÉRIQUE, 2017, p. 3).

> field of digital arts (STRATÉGIE INTERNATIONALE DE LA FRANCE POUR LE NUMÉRIQUE, 2017, p. 27, own translation)[73]

In this statement, one can recall elements of strategic autonomy in the French mentality. These elements appear more explicitly in the document when it states: "France will continue to guarantee its strategic autonomy by maintaining the necessary industrial, scientific and technical capacities" (STRATÉGIE INTERNATIONALE DE LA FRANCE POUR LE NUMÉRIQUE, 2017, p. 31, own translation)[74].

Also relevant is that the subtle threat landscape raised the peril of a fragmented Internet. The strategy points to "Authoritarian states, anxious to assert their sovereignty over the digital world, seek control of networks, to the detriment of the openness that constitutes its foundation and at the expense of fundamental rights" (STRATÉGIE INTERNATIONALE DE LA FRANCE POUR LE NUMÉRIQUE, 2017, p. 4, own translation)[75]. In this regard, France's international strategy acknowledges that the transnational character of cyber issues demands the country to "integrate a European and international dimension into its efforts" (STRATÉGIE INTERNATIONALE DE LA FRANCE POUR LE NUMÉRIQUE, 2017, p. 30, own translation)[76], particularly citing the European Union and NATO. In this sense, the country reinforced its aim to "ensure the integration of cyber defense into the military operations of the European Union and NATO" (STRATÉGIE INTERNATIONALE DE LA FRANCE POUR LE NUMÉRIQUE, 2017, p. 31, own translation)[77].

The incorporation of an international engagement and the perception of a real risk of Internet fragmentation caused one interesting behavior in France. It formally set the post of a

[73] From the original in French: "La France entend, à cet égard, promouvoir sa vision du numérique, que ce soit en matière de transformation numérique de l'État, d'ouverture des données publiques ou de protection des données personnelles, tout en développant des écosystèmes ouverts, depuis lesquels les start-up françaises pourront rayonner au-delà de nos frontières et dans lesquels seront accueillis des entrepreneurs, des talents et des investisseurs venus du monde entier. Il s'agit également d'explorer et de promouvoir toutes les nouvelles formes de création (transmédia, arts numériques, nouvelles écritures, etc.) et de valoriser la création française dans le domaine des arts numériques" (STRATÉGIE INTERNATIONALE DE LA FRANCE POUR LE NUMÉRIQUE, 2017, p. 27).

[74] From the original in French: "a France continuera à garantir son autonomie stratégique par le maintien des capacités industrielles, scientifiques et techniques nécessaires. (STRATÉGIE INTERNATIONALE DE LA FRANCE POUR LE NUMÉRIQUE, 2017, p. 31).

[75] From the original in French: . Les États autoritaires, soucieux d'affirmer leur souveraineté sur le monde numérique, recherchent le contrôle des réseaux, au détriment de l'ouverture qui en constitue le fondement et aux dépens des droits fondamentaux "(STRATÉGIE INTERNATIONALE DE LA FRANCE POUR LE NUMÉRIQUE, 2017, p. 4).

[76] From the original in French: "la France doit également intégrer une dimension européenne et internationale à ses efforts. (STRATÉGIE INTERNATIONALE DE LA FRANCE POUR LE NUMÉRIQUE, 2017, p. 30).

[77] From the original in French: " La France veillera également à l'intégration de la cyberdéfense aux opérations militaires de l'Union européenne et de l'OTAN" (STRATÉGIE INTERNATIONALE DE LA FRANCE POUR LE NUMÉRIQUE, 2017, p. 31).

digital ambassador in 2018[78]. Besides, France started to push for collective support from like-minded countries. An example of this movement was the Paris Call for Trust and Security in Cyberspace, a document calling for stakeholders to come together to face the new threats endangering citizens and infrastructure based on nine principles.[79]

France also built a more robust agenda domestically, with the Strategic Review of Cyber Defense setting seven main principles to France's ambition in cyber defense:

> - place priority on protecting our information systems;
> - adopt an active stance of attack deterrence and coordinated response
> - fully exercise our digital sovereignty
> - provide an effective penal response to cybercrime
> - promote a shared culture of information security
> - help to bring about a digital Europe that is safe and reliable
> - act internationally in favor of a collective and controlled governance of cyberspace
> (SGDSN, 2018a, p. 3).

In this regard, the Strategic review exposes further ideas regarding strategic autonomy. It reinforces the idea of the polyform character of threats, encompassing espionage, illicit traffic, destabilization, and sabotage (SGDSN, 2018b, p. 11).

More relevant, though, is that the English version of the Strategic Review is more condensed than the original document in French. Therefore, the English translation recognizes power relations occurring in cyberspace exist, pointing to the complexity of these relations caused by the "ambiguous roles of Google, Apple, Facebook, and Microsoft (GAFAM)"(SGDSN, 2018a, p. 4). While the french version clearly explains France's vision of what power in cyberspace means:

> The power of a state in the cyber domain is not measured by the mere possession of offensive and defensive capabilities. It is fundamentally based on the latter's ability and willingness to use them fully. It depends on the determination to deter attacks by increasing the difficulty, cost, and risk to an attacker. Finally, it assumes that the State can rely on an industry able to relay and expand its action. It is now up to France to take up this challenge of cyber power. (SGDSN, 2018b, p. 43, own translation)[80].

[78] Which was assigned a defined scope of action in a mission letter and validated interministerial on 3 June 2019 (FRANCE DIPLOMATIE, 2022).

[79] The nine Paris Call principles are: Protect Individuals and Infrastructure, Protect the Internet, Defend ElectoralPprocess, Defend Intellectual Property, Non-Proliferation, Lifecycle Security, cyber Hygiene, Non-Private Hack-Back, and International norms (PARIS CALL, 2022).

[80] From the original in French: "La puissance d'un Etat dans le domaine cyber ne se mesure pasà la seule possession de capacités offensives. Elle repose fondamentalementsur l'aptitude et la volonté de celui ci des employer pleinement. Elle dépend de la détermination à décourage les attaquesen augmentant la difficulté, le côut et le risque pour un agresseur. Elle suppose, enfin, que l'État puisse s'appuyer sur une industrie em mesure de relayer ou d'élargir son action. Il appartient aujourd'hui à la France de relever ce défi de la cyberpuissance" (SGDSN, 2018b, p. 43).

Thus, France's vision of power relations in cyberspace encompasses both "power to control" when it mentions the ability to deter attackers and the idea of a "protean power" since it attaches industrial capacity (innovation) to the equation.

Besides, the original document explains France's six cyber defense missions: prevention, anticipation, protection, detection, attribution, and reaction (remediation, repression of offenses, and military actions) (SGDSN, 2018b, p. 48). This idea would base the French Cyber Defense Policy (*Politique ministérielle de lutte informatique défensive* – LID).

The Cyber Defense Policy would mainly cover three missions: anticipate, detect, and react, complementing thus the other three: prevent, protect and assign (MINISTÈRE DES ARMÉES, 2019a, p. 5). Moreover, prevention and protection actions would concern MoD's computer systems (friendly zone). While anticipation, detection, and reaction missions would focus on computer systems belonging to other categories of actors (neutral and enemy zones) (MINISTÉRE DES ARMÉES, 2018, p. 9). In this sense, the COMCYBER would plan LID operations in coordination with ANSSI, the intelligence services, “and possibly other partners (national or international)” (MINISTÈRE DES ARMÉES, 2019a, p. 5, own translation).[81]

Interestingly, the Cyber Defense Policy reinforced France’s perception of cyberspace as a "confrontational environment for States or non-governmental organizations in which the risk of attack is considered permanent, including in times of peace." Thus, the need for a permanent cyber defense posture (PPC). In other words, a posture placed under the command of COMCYBER that "consists of all the provisions adopted to permanently ensure (24/7) the defense of the Ministry's IT systems in the peace-crisis-war continuum" (MINISTÈRE DES ARMÉES, 2019a, p. 9, own translation)[82]. In this sense, cyberspace is set as a place of opportunities and vulnerabilities for France. With a proper dynamic and as an efficiency multiplier, “as long as we have the right data and information, which have become a critical resource at the heart of the political, economic and social functioning of modern societies” (MINISTÈRE DES ARMÉES, 2019a, p. 3, own translation)[83].

[81] From the original in French: “et éventuellement d’autres partenaires (nationaux ou internationaux)” (MINISTÈRE DES ARMÉES, 2019a, p. 5).

[82]From the original in French: “Le cyberespace est un milieu de confrontation pour les Etats ou les organisations non gouvernementales dans lequel le risque d’attaque est considéré comme permanent, y compris en temps de paix (…) La PPC est constituée de l’ensemble des dispositions adoptées pour assurer en permanence (24h/7j) la défense des systèmes informatiques du ministère dans le continuum paix-crise-guerre” (MINISTÈRE DES ARMÉES, 2019a, p. 9).

[83]From the priginal inFfrench: “pour peu que l’on dispose des bonnes données et informations, qui sont devenues une ressource critique, au coeur du fonctionnement politique, économique et social des sociétés modernes” (MINISTÈRE DES ARMÉES, 2019a, p. 3).

One year after the launch of LID, the Ministry of Defense, Florence Parly, affirmed that France was using and would use cyberweapons (*arme cyber*) in military operations (VIE PUBLIQUE, 2019). Furthermore, the Cyber Offensive Military Doctrine (*Doctrine Militaire de Lutte Informatique Offensive* – LIO) was made partially public. The Offensive Cyber Doctrine expressed that “most contemporary power struggles, crises, and conflicts develop in the digital space” (MINISTÈRE DES ARMÉES, 2019b, p. 4, own translation)[84]. Besides, it set the guidelines for LIO, which was designed to cover "all actions undertaken in cyberspace, conducted independently or in combination with conventional military mean" (MINISTÈRE DES ARMÉES, 2019b, p. 5, own translation)[85].

The public doctrine emphasized that cyber weapons would aim “in strict compliance with international rules, to produce effects against an adverse system to alter the availability or confidentiality of data” (MINISTÈRE DES ARMÉES, 2019b, p. 5, own translation)[86]. The document also expressed that LIO would take its full dimension of potential multiplier effects (amplifying, improving, or supplementing) if combined with conventional military means (MINISTÈRE DES ARMÉES, 2019b, p. 6). Besides, the doctrine exposed that LIO could produce material and immaterial effects. The first was related to neutralizing a weapon system, while the latter was related to intelligence gathering. In this regard, the document reinforced the perception of cyber operations as a force multiplier. Still, acknowledging immaterial effects can also represent an agreed vision of cyber operations having merit on their own.

Interestingly, within the Cyber Offensive Doctrine, France recalled its commitment to NATO in the Cyber Defense Pledge of 2016[87]. Moreover, the country's leading role within Europe is "in the promotion of a shared cyber military culture and aims to develop the means of operational interoperability with our main European partners" (MINISTÈRE DES ARMÉES, 2019b, p.10, own translation)[88]. Besides, LIO employment, as in conventional military operations, would imply the “acceptance of the risk by the decision-making level,

[84] From the original in French: “La plupart des luttes de pouvoir, des crises et des conflits contemporains connaissent un développement dans l’espace numérique” (MINISTÈRE DES ARMÉES, 2019b, p. 4).

[85] From the original in French: “La lutte informatique offensive à des fins militaires (LIO) recouvre l’ensemble des actions entreprises dans le cyberespace, conduites de façon autonome ou en combinaison des moyens militaires conventionnels” (MINISTÈRE DES ARMÉES, 2019b, p. 5).

[86] From the priginal in French: “ L’arme cyber vise, dans le strict respect des règles internationales, à produire des effets à l’encontre d’un système adverse pour en altérer la disponibilité ou la confidentialité des données” (MINISTÈRE DES ARMÉES, 2019b, p. 5).

[87] The Cyber Defense Pledge was a commitment of member countries to equip themselves with cyber resources to ensure their individual and collective security (NATO, 2016).

[88] From the original in French: “ rôle moteur dans la promotion d’une culture militaire cyber partagée et ambitionne de développer les moyens d’interopérabilité opérationnelle avec nos principaux partenaires européens” (MINISTÈRE DES ARMÉES, 2019b, p.10).

determined by the principles of *jus in bello.*[89] (proportionality, distinction, discrimination, etc.) (MINISTÈRE DES ARMÉES, 2019b, p. 9). In this regard, the application of international law to cyberspace was already being specified by France.

Notwithstanding, to delving into a national understanding of the applicability of International law to cyberspace, France had a proactive initiative to publish a document on the subject (*Droit International Appliqué aux Opérations dans le cyberspace*). The document revolves around key issues under discussion internationally, such as liability, attribution, and proportional response. In this regard, it is interesting that for France, "A cyberattack causing damage of a significant scale and seriousness may constitute an armed attack giving rise to the right to use self-defense" (MINISTÈRE DES ARMÉES, 2019c, p. 8, own translation)[90]. In other words, the cyber attack would need to "cause substantial human losses, or considerable physical or economic damage" to be considered an armed attack (MINISTÈRE DES ARMÉES, 2019c, p. 9, own translation)[91]. In this regard, France adopts a view that cyberspace can result in actions involving the use of force. Thus coercion as an element of "power to control" appears.

Still, in the international realm, one alliance calls attention. On 22 January 2019, a bilateral cooperation treaty (on a level of the Élysée Treaty.[92]) was signed between ANSSI and its German counterpart, the German Federal Office for Information Security(*Bundesamt für Sicherheit in der Informationstechnik* – BSI) (ANSSI; BSI, 2019). This treaty and the development of several joint projects between Germany and France indicate a further replication of a political-economic engine driven by the two countries within the European Union context.

Domestically, two document updates call the attention. The first is the update of the National Intelligence Strategy (*La stratégie nationale du renseignement*) that, in its first version, mentioned cyberattacks among the threats but in its updated version recognized, "even more explicitly, the place of cyberspace and devotes a long development to it in the presentation of the priority issues of the intelligence, as part of the fight against cross-cutting

[89] Jus in bello regulates the conduct of parties engaged in an armed conflict, being a synonym for International Humanitarian Law (ICRC, 2015).

[90]From the original in French: "Une cyberattaque provoquant des dommages d'une ampleur et d'une gravité significatives peut constituer une agression armée ouvrant le droit de faire usage de la légitime défense (MINISTÈRE DES ARMÉES, 2019c, p. 8).

[91]From the original in French: " Une cyberattaque pourrait être qualifiée d'agression armée dès lors qu'elle provoquerait des pertes humaines substantielles, ou des dommages physiques ou économiques considérables" (MINISTÈRE DES ARMÉES, 2019c, p. 9).

[92]The Élysée Treaty was signed 18 years after the Second World War, aiming to represent a lasting commitment between France and Germany "that went beyond any future political changes and to make their cooperation official and systematic" (FRANCE DIPLOMACY, 2022).

threats" (CAMBON, 2020, p. 239-240, own translation)[93]. The second is the update on the Military Planning Law (LPM 2019-2025), which strengthened the armed forces' capabilities in preventing, detecting, and attributing cyberattacks. It dedicated an additional 1.6 billion euros for cyber operations and 1,500 additional personnel for 4,000 cyber combatants by 2025 (LAUDRAIN, 2019b).

In 2020 the COVID -19 pandemic would boost malicious cyber activity and thus impact France's threat perceptions. According to the 2019-2020 DPR's annual report, new tendencies in cyberspace appeared. The first tendency relates to the accessibility of attack tools, given its growth in the Darkweb, "which lowers the cost of the initial investment and makes, in fact, the number of attackers always more important." The second tendency relates to social engineering. As sponsored attackers (especially those sponsored directly or indirectly by the States), in search of accessing its increasingly protected targets, seek to reach the weaker links. The third tendency relates to the attackers "increasing sophistication of *modus operandi* aimed at concealing their real origin and disorienting attack attribution capabilities" (CAMBON, 2020, p. 243, own translation)[94].

The third edition of the Franco-German common situational picture further exposed two significant threat actors: State or state-level actors and cybercriminals. The first threat would encompass actors focusing mainly on cyber espionage, destabilization, or sabotage. In contrast, the second would contain financially motivated actors and be responsible for a greater number of attacks (ANSSI; BSI, 2020, p. 2). According to ANSSI, the years 2019-2020 were marked by an explosion of ransomware (ANSSI, 2022b). Besides, the Agency exposed that 2019 saw an increase in indirect cyber-attacks through the exploitation of supply chains and that “geopolitical tensions have also prompted operations of pre-positioning of malicious codes, system recognition, even sabotage” (ANSSI, 2020a, p. 34, own translation). In this context, ANSSI’s Manifest attested that the “mastery of cyberspace is becoming one of the keys to power in the world to come” (ANSSI, 2020b, p.10, own translation)[95].

Still, in the pandemic scenario, ANSSI's IT Threat Overview 2021 (*Panorama de la Menace Informatique 2021*) indicated that cyber espionage remained the main purpose pursued by state attackers. According to the document, of ANSSI's 17 cyber defense

[93] From the original in French: “(…) reconnaît, encore plus explicitement la place du cyberespace et lui consacre un long développement dans la présentation des enjeux prioritaires du renseignement, au titre de la lutte contre les menaces transversales” (CAMBON, 2020, p. 239-240).

[94] From the priginal in French: “La troisième est la sophistication croissante des modes opératoires visant à dissimuler leur origine réelle et désorienter les capacités d’attribution des attaques” (CAMBON, 2020, p. 243).

[95] From the original in French: “(…) la maîtrise du cyberespace devient l’une des clés de puissance dans le monde à venir” (ANSSI, 2020b, p. 10).

operations, 14 were linked to cyber espionage operations. The document also noted that cyber-attacks using influence and destabilization operations were anticipated, particularly in the run-up to major events in France (ANSSI, 2022c).

The latest threat assessment led France's MoD to publish 2021 a new strategic update in which it recognized the emergence of "new domains for the expression of power (cyber, space)" (MINISTÈRE DES ARMÉES, 2021a, p. 24). The document further exposes that "the emerging confrontations with regional and major powers confirm the need to continue strengthening the capabilities of the armed forces to operate in cyberspace and exploit technical intelligence" (MINISTÈRE DES ARMÉES, 2021a, p. 41). Besides, it acknowledged the importance of securing supply chains and emerging technology fields (AI, hyper-velocity, stealth, cyber including networks, control of the electromagnetic environment, combat cloud, nanotechnology, etc.).Thus, the need to better coordinate defense efforts within the EU, generating high technology and industrial independence, given the extended economic confrontation to new areas of competition (MINISTÈRE DES ARMÉES, 2021a). The proposed independence thus would include cyberspace and emerging technologies.

Besides the Strategic Update, the launch of the Cyber Influence Warfare Doctrine (*Doctrine Militaire de Lutte Informatique d'Influence* -L2I) in 2021 set the third step of MoD to complete its strategy toward cyber defense since it could be employed along with LIO and LID. In this regard, the document set a framework for "military operations conducted in the information layer of cyberspace to detect, characterize and counter-attacks" and undertake "intelligence gathering or deception operations" (MINISTÈRE DES ARMÉES, 2021b, p. 9, own translation)[96].

The L2I doctrine explains that cyberspace would be the new space for information warfare. According to the document, cyberspace has become the terrain of deception operations "and for some actors the terrain of disinformation operations" (MINISTÈRE DES ARMÉES, 2021b, p. 6, own translation)[97]. In this sense, it poses the following threats: organized armed groups, terrorist armed groups, and quasi-states "that exploit informational leverage for propaganda, financing, recruitment or coordination purposes to harm their adversaries" (MINISTÈRE DES ARMÉES, 2021b, p. 7, own translation)[98]. It further recalls

[96] From the original in French: " de recueil de renseignement et d'opérations de déception qui doivent être pleinement exploitées (MINISTÈRE DES ARMÉES, 2021b, p. 9).

[97] From the original in French: "et pour certainsacteurs le terrain d'opérations de désinformations"(MINISTÈRE DES ARMÉES, 2021b, p. 6).

[98] From the original in French: "des structures étatiques ayant pour finalité, lorsqu'elles ciblent des États, de les déstabiliser, de fragiliser leur cohésion ou encore de discréditer les pouvoirs publics" MINISTÈRE DES ARMÉES, 2021b, p.7).

France's engagement in EU and NATO contexts on its support of initiatives to combat the manipulation of information (MINISTÈRE DES ARMÉES, 2021b, p. 13).

Following its concern over independence on supply chains and emerging technologies, France launched its *France Relance* plan, strengthening France's digital sovereignty through greater mastery of strategic digital technologies and support for business development as a priority. The plan thus set the amount of 1.7 billion euros for investments in the digital transformation of the state and the territories, being 136 million euros devoted to cybersecurity over the period 2021-2022, and entrusted to ANSSI (ANSSI, 2022d). This effort shows a continuum of France's investment toward cybersecurity. Since the ANSSI's budget started in 2010 at € 43 million, it grew to 83,8 million in 2014, reaching € 100 million in 2017 (DESFORGES, 2018).

Financed by the *France Relance* Plan as well as the future investment program (PIA) [99] , the National Strategy for Cybersecurity Acceleration (*Stratégie nationale d'accélération pour la cybersécurité*) was launched in 2021. Mobilizing, thus, €1 billion, including €720 million from public investments, the strategy was about to bring French cybersecurity champions and address the trust issue. It articulates around four axes:

a) Developing sovereign and innovative cybersecurity solutions.
b) Develop cybersecurity to strengthen links and synergies between industry players.
c) Strengthen the industry.
d) Support demand (individuals, companies, local authorities, and the State) by raising French people's awareness of cybersecurity while promoting national offers.
e) Train more young people and professionals in cybersecurity professions (GOUVERNMENT, 2021).

In this regard, France's perception of cyberspace dynamics appears to have been pushed to seek better relationships with the private sector. Thus, one of the structuring programs for cybersecurity is Campus Cyber. The Campus was launched at the beginning of 2022 to welcome and promote collaboration between companies, State services, research actors, and training organizations and associations (CAMPUS CYBER, 2022). This initiative

[99] "The Future Investments Program (PIA), steered by the General Secretariat for Investment (SGPI), was set up by the State to finance innovative and promising investments in the territory in order to enable France to increase its potential for growth and jobs. From the emergence of an idea to the distribution on the market of a new product or service, the PIA intervenes throughout the life cycle of innovation. It links public research and the world of 'business. The PIA is based on a dual principle of leverage and risk sharing: State investment in an innovation project is most of the time co-financed by private or public partners. Since the launch of the PIA, the State has thus co-financed several thousand projects to prepare for the future" (GOUVERNMENT, 2018, own translation).

consolidates France's holistic approach to cybersecurity and cyberdefense and is a concrete, practical example of the global approach set in 2014.

4.2 CYBER POWER PERCEPTIONS

The document analysis showed the context that caused France's change of digital mentality over the years. From needing to catch up to a “Digital Republic,” one can notice that the French global approach has more recently given some subtle indications of what power in cyberspace means and its very existence. A synthesis of the evidence by the strategies produced in each period can be seen in Table 10.

Notwithstanding, some critical perceptions over the topic become more straightforward with the answers interviewees. Given the centrality of France's cybersecurity and defense framework in ANSSI and MoD, there was an attempt to contact someone from both agencies. Regarding ANSSI, no answer from the Agency was obtained in due time of the research. The MoD agreed to participate with written answers (Interviewee B). Besides these agencies, contact with the MFA was made. This contact resulted in the interview of a cyber-diplomat (Interviewee C).

Table 10 - France’s Digital Mentality Summary

NCSS	Orientation	Threats Perceived	Self Perception	Investment (ANSSI)	Conventional Power Elements
2011	Techno-military approach	Foreign states (espionage) Terrorists Criminals* (not much relevance to national security)	Emerging cyberdefense power	€ 43 million	Military Economic Informational Diplomatic Political
2015	Global approach	Foreign states Terrorists Criminals Big Digital Platforms	Digital Republic and cyber defense power	€ 83,8 million	Military Economic Informational Diplomatic Political

Source: Own elaboration based on France’s National Cyber strategies and Desforges (2018).

In MoD's answers, one can observe the aversion to using the word cyber power, interpreting it as the power to control and gain dominance. Interviewee B (2020) reinforced that "France does not intend to take a dominant stance over any other country when asked about perceptions of power in cyberspace." Besides, when asked about actors' capacity for achieving power in cyberspace, it stated, "This is not a matter of discussion within the French MoD, as there is no strategy to express power in the cyberspace."

In this regard, the answer of some questions raised France's cyber defense discussion. Interviewee B (2020) states: "As cyber power does not mean anything from a French perspective, I would use the French cyberdefence capabilities as a reference” when asked to rank France's cyber power position." In this context, when asked about defensive and offensive cyber operations, Interviewee B (2020) stated that offense and defense would be the "two sides of any defence policy and cyberdefence is organized accordingly." Besides answering about France's position internationally and regionally, the interviewee stated, "Let us say that France belongs to the major actors of cyberdefence, clearly above the average, but with some limitations due to our demography."These answers resonate with the documents on a preference for a defensive approach from France without ruling out a stronger (offensive) response if needed.

Moreover, if the documents raised the importance of strategic autonomy to be used in cyberspace for France, one answer of Interviewee B reinforced it. When asked about elements for the maintenance of cyber power, the answer was, "Any state which intends to keep a reasonable cyberdefence capability needs an IT industry able to support this policy" (INTERVIEWEE B, 2020). The innovation and autonomous industrial capacity element are very much present in this answer and the last couple of years with the initiatives described in the previous subsection.

Similarly, Interviewee C (2020) pointed out that to be a strong country in cybersecurity, four elements would be important: capacities (both offensive and defensive, plus attribution capability), a clear doctrine (both in its physiology and actions), a good administration, and an innovation ecosystem. In this sense, Interviewee C also avoided using the term "cyber power," clarifying that answers would be in a cybersecurity context. Interviewee C (2020) mentioned that France had a very defensive view over cyberspace, trying to be a "canon for deterrence" and claiming that the "best defense is defense."

Along with the interview, the subject of sovereignty was also brought up. Thus, Interviewee C (2020) explained that France seeks to fight for a "free, open, secure, and unique Internet," promoting a multistakeholder approach where sovereignty must be in a “democratic context." In this regard, Interviewee C (2020) linked sovereignty to citizen's rights protection, especially digital privacy. Besides, Interviewee C (2020) stressed that France would not rely upon allies to react to cyber-attacks. Instead, it would act based on evidence from its own analysis (regardless of when it would be necessary for it to be established) and respect International Law.

In further explaining the multistakeholder approach, Interviewee C (2020) highlighted that the clear division between security and defense among agencies (involving ANSSI and MOD) was considered a strength since it provided a more transparent environment to work with the private sector. In fact, in Interviewee C's view, "The more you build a strong state, the more you need to pen it." Therefore, one can infer that transparency would be a key element in the French multistakeholder approach.

The cyber diplomat explained that "states do not understand how the Internet works and alone they would be making huge mistakes," thus the need to engage government, companies, and civil society. Notwithstanding, Interviewee C (2020) emphasized that companies' capacities would not make them sovereign entities. Thus, France discouraged them from acting in contexts of "hack-back" and engaging in state matters, such as war and International Law. This observation recalls the restraint on digital platforms monopolies expressed in France's cyber strategy.

Another highlight amid the answers was that although advocating for a cyberspace "governance" international configuration, Interviewee C (2020) acknowledged that states have different capabilities degrees. Thus, one can think in a more hierarchical structure. Still, France would put its efforts in opposition to establishing one unique super(cyber)power. In this context, it was relevant that Interviewee C (2020) positioned France internationally in an intermediary rank, considering its influence and capabilities. Interviewee C (2020) further explained that "like few countries, we [France] have a very serious administration," and inside Europe, France was one of the leaders in cybersecurity.

Interestingly, when asked about "cyber power maintenance," Interviewee C (2020) recalled Europe. In this regard, the cyber diplomat stated that France was proposing that Europe take a multistakeholder approach to form a strong coalition and be a real geopolitical actor. In this sense, by stressing the importance of a relevant political Europe, one can recall another element of strategic autonomy transposed to the cyber realm by France.

The interviews reinforced some elements the official documents and legislation analyzed pointed out. Still, they highlighted some subjective perceptions regarding the term "cyber power," showing concern over how it could be interpreted as a synonym for dominance or against a multistakeholder approach.

4.3 PARTIAL CONCLUSIONS

The chapter showed that France varied its cybersecurity approaches in two main directions: techno-military and global. This variation reinforces France's threat and self-perceptions, demonstrating an evolution of the state's digital mentality, grounded deeply in ideas related to strategic autonomy. In this regard, France's digital mentality led the country to assume a more active, still discreet, position toward cyberspace. In this sense, the chapter interestingly displayed France's perception of cyber as a force multiplier while having concerns over the term cyber power itself.

5 GERMANY’S DIGITAL MENTALITY AND CYBER POWER PERCEPTION

The present chapter presents Germany’s digital mentality evolution through time and the state’s perception of power and cyberspace along this evolution. In other words, it tracks the changes in Germany’s self-perception and threat perceptions. Thus, the chapter is divided into three subsections: general context and the phases of Germany’s digital mentality, interviews inputs on cyber power perceptions, and partial conclusions.

5.1 GERMANY’S DIGITAL MENTALITY

In Germany, issues related to Information Technology (IT) security started to gain attention in the early 1980s. In West Germany, an association founded in 1981 called Chaos Computer Club (CCC)[100] had an active hacking community, and successful hacking attacks brought attention to the broader public (SCHALLBRUCH; SKIERKA, 2018). Hacking at this time was seen more as a disruptive and ludic activity, sometimes motivated by financial gains, than a severe national threat.

The government's concern of criminalizing such activities, even if done early on, 1986 in the penal code, "only criminalized the theft of data, but not the intrusion into a system under surpassing security precautions" (SCHALLBRUCH; SKIERKA, 2018, p.6). Steiger points out that despite the early acknowledgment of the economical relevance of data and the growing dependency of companies and public administration on IT, a proposal for making secure data a punishable offense was prevented. This was because there was a strong view that hackers dealing “with the mere intrusion” of content in a computer system, for example, should be spared from punishment (STEIGER, 2022, p. 158, own translation)[101]

The acknowledgment of IT relevance also resulted in 1986 in the creation of the Central Office for Encryption (*Zentralstelle für das Chiffrierwesen* – ZfCh). It was set up as a working party to deal with security questions. Only one year after the reunification (*Wiedervereinigung*) in January 1991, ZfCH gave space to the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* -BSI). BSI is a subsidiary agency within the Ministry of Interior (*Bundesministerium des Innern und für Heimat* - BMI) (ROMANIUK; CLAUS, 2021), which “began work as an offshoot” of the Federal

[100] CCC still exists today and is Europe's largest association of hackers (CCC, 2022).
[101] From the original in German “Hackers, die sich mit dem bloßen Eindringen”.

Intelligence Service, Germany’s foreign intelligence agency (*Bundesnachrichtendienst*-BND) (BEIGEL; HERPIG, 2021, p.11).

In this sense, BSI became responsible for strengthening the security of the government's information technology and ensuring government networks' protection, showing a technically driven approach to the issue. Just three years after BSI’s creation, the national Computer Emergency Response Team (CERT-Bund) was set up (BSI, 2022a). It was designed to be “the central point of contact for preventive and reactive measures in the event of security-related incidents in computer systems”[102] (BSI, 2022b, own translation).

Along with the first steps toward a cybersecurity institutional architecture, Germany started to perceive the complexity of cyberspace interactions. In 1998 a Commission was formed to present the political consequences resulting from the use of the new information technologies, name the need for government action and propose parliamentary initiatives (BÖHLE, 1996). The Commission of Inquiry Future of the Media in Economy and Society – Germany's way into the information society (*Enquete-Kommission Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft*) pointed in its final report that new types of threats would be coming from the globally interconnected systems of electronic communication (DEUTSCHER BUNDESTAG, 1998).

In this regard, the report exposed that:

> Threats can come from individual criminals, terrorists, criminal organizations, or even enemy states. In this respect, the distinction between civil and military threats and between internal and external security is becoming increasingly blurred.
>
> Attacks on the information infrastructure are based on means and methods of information- and program-controlled disruption and destruction of the functionality of civil and military communication and command systems. Computer-assisted disruption and destruction of files of this type are also referred to as "cyber wars" (DEUTSCHER BUNDESTAG, 1998, p. 84, own translation).[103]

[102] From the original in German: “CERT-Bund, das Computer Emergency Response Team für Bundesbehörden, ist die zentrale Anlaufstelle für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen in Computer-Systemen”.

[103] From the original in German: “Bedrohungen können von kriminellen Einzeltätern, von Terroristen, von kriminellen Organisationen oder auch von feindlichen Staaten ausgehen. Insofern wird die Unterscheidung zwischen ziviler und militärischer Bedrohung sowie zwischen innerer und äußerer Sicherheit immer verschwommener.

Die Angriffe auf die Informationsinfrastruktur stützen sich auf Mittel und Methoden der informations- und programmgesteuerten Störung und Zerstörung der Funktionsfähigkeit ziviler und militärisch genutzter Kommunikations- und Führungssysteme.Computergestützte Störungs- und Zerstörungsakte dieser Art werden auch als "Cyberwar" bezeichnet“ (DEUTSCHER BUNDESTAG, 1998, p. 84).

Besides, it demonstrated an early concern with gray zones between military and civil spaces[104] and some attention devoted to critical infrastructures. This is clear when it explains that defensive measures "must in future be based on the system monitoring and technical-organizational system adjustment in the areas of the state and international information infrastructures"[105] (DEUTSCHER BUNDESTAG, 1998, p. 84-85, own translation).

Besides, although considering hacking intrusions a light threat, Germany fostered a considerable debate on privacy protection through cryptography. According to Steiger (2022, p.160), cryptography for the protection of communications would be a "crystallization point"[106] in German's Cyber Security Policy. The concern over cryptography culminated in 1999 with a Crypto Policy *(Eckpunkte der deutschen Kryptopolitik*) (STEIGER, 2022, p.168). In this sense, Germany strengthened BSI's scope to ensure secure encryption. According to Herpig and Heumann (2017, para 4), five core elements are present in the document. These are:

> 1. There will be no ban or limitation on crypto products
> 2. Crypto products shall be tested for their security in order to increase the user's trust in those products
> 3. The development of crypto products by German manufacturers is essential for the country's security, and their ability to compete internationally shall therefore be strengthened
> 4. The widespread use of encryption shall not weaken law enforcement and security agencies. The development of additional technical competencies for those agencies shall be fostered
> 5. International cooperation on crypto issues such as open standards and interoperability is vital and shall be fostered bi- and multilaterally.

In this regard, one can notice a transfer from Germany's memory on the need for data protection and privacy in the digital sphere. Nazism and, later on, the Stasi secret police[107] imposed a robust surveillance regime in East Germany, marking Germans attached to data protection and privacy (SCHALLBRUCH; SKIERKA, 2018).

In this context, one can highlight an initial link to the informational sphere (i.e., content) itself with IT security debates, mainly because BSI's mandate included the promotion

[104] The report states: "Insofern wird die Unterscheidung zwischen ziviler und militärischer Bedrohung sowie zwischen innerer und äußerer Sicherheit immer verschwommener" (DEUTSCHER BUNDESTAG, 1998, p. 84).

[105] From the original in German: "Alle diese Maßnahmen müssen in Zukunft auf die Systemüberwachung und technisch-organisatorische Systemanpassung in den Bereichen staatlicher und internationaler Informationsinfrastrukturen übertragen werden".

[106] From the original in German: "Kristallisationspunkt".

[107] "The Nazi regime systematically abused private data for the identification and persecution of Jews, homosexuals, political opponents, and other groups. East Germany functioned as a socialist dictatorship in which the Stasi ran a nationwide surveillance regime that relied on denunciation and electronic surveillance" (SCHALLBRUCH; SKIERKA, 2018, p. 2).

of secure encryption. Still, the main driver of the German approach to the digital domain remained technical, reinforcing a preference to treat cybersecurity from a technical perspective.

The technical perception, thus, would follow the first developments of Germany's digital mentality. However, unlike France, it would be intertwined with a civil approach since the military was not engaged directly in IT security discussions at this stage.

5.1.1 The first phase (2005-2015): Techno-civilian approach

The beginning of the 2000s led to a broader discussion within Germany on IT reliability. After the incident related to the spread of the Loveletter virus through E-mail attachments, a "first intensive debate about cybersecurity in the German Bundestag" happened (SCHALLBRUCH; SKIERKA, 2018, p.6). In this regard, 2005 was a pivotal year for the country since the president of BSI "penned a report in which he reasoned that Germany needed to seriously consider integrating cyber security into the state's national security calculus" (ROMANIUK; CLAUS, 2021 p.73).

Considering the recommendation and acknowledging the need for improvement in the protection of IT systems in Germany's most critical infrastructures,[108] the National Plan for the Protection of Information Infrastructure (*Nationaler Plan zum Schutz der Informationsinfrastrukturen*- NPSI) was developed and launched.

NPSI defines IT security as "the condition that ensures the availability, integrity, liability, and confidentiality of information when using IT" (BMI, 2005, p.20, own translation)[109]. Based on this definition, the document acknowledged that criminals and terrorists were "increasingly attempting to damage the complex technical systems through targeted attacks." It further points out, "It cannot be ruled out that vital information infrastructures in Germany will also become the object of targeted attacks" (BMI, 2005, p.3, own translation)[110]. Thus, the document set three main goals to protect Germany’s critical infrastructure:

[108] This acknowledgment was reached after a series of studies that were the result of two significant events that impacted Germany's threat perception: the USA 9/11 terrorist attacks and the 2004 denial of service (DoS) attack on the federal government's networks (SCHALLBRUCH; SKIERKA, 2018, p. 8).

[109] From the original in German: “IT-Sicherheit ist der Zustand, der die Verfügbarkeit, die Integrität, die Verbindlichkeit und die Vertraulichkeit von Informationen beim Einsatz von IT gewährleistet” (BMI, 2005, p. 20).

[110] From the original in Germna: “Immer häufiger versuchen auch Kriminelle und Terroristen, die komplexen technischen Systeme durch gezielte Angriffe zu schädigen. Es ist nicht auszuschließen, dass auch

a) To adequately protect information infrastructures (Prevention)
b) To act effectively on IT security incidents (Response)
c) To strengthen German IT security competence by setting international standards (Sustainability).

Interestingly, NPSI exposes that its cornerstones were the cooperation with companies and "active inclusion of German interests in political decision-making at the international level." (BMI, 2005, p. 9, own translation)[111]. Thus, from the beginning of its digital mentality development, one can infer that Germany saw the international realm as an important action area. It is vital to notice that despite mentioning an active role, no assertive measures are detailed. Instead, the document emphasized a soft approach grounded in cooperation in the international arena, following Germany's broad Foreign Policy reasoning.

The document further explained the importance of BSI, indicating its competencies and tasks would be expanded along the course of NPSI implementation. Besides, it highlights that it would be "essential for the security of the German information society and Germany as an industrial location that innovative, trustworthy crypto products are available to ensure confidential communication" (BMI, 2005, p.11)[112]. In this regard, securing Germany's position as an international industrial reference is relevant and concerned with maintaining its economic power status, especially within Europe. Therefore, one can infer that a link between security and the economy was being cultivated in Germany's digital mentality.

After the launch of the NPSI, another essential document would mention the relevance of IT security for the country: the White Paper. The 2006 White Paper (*Weißbuch*) pointed out in the section "The strategic framework –Global challenges, opportunities, risks and hazards" the downside of the free information and ideas exchange proportioned by globalization. It would be "the risk of illicit acquisition and misuse of sensitive knowledge, technologies and new capabilities by states, non-state actors, international terrorism or organized crime." Therefore, as its critical infrastructure, Germany's political and economic structures became

lebenswichtige Informationsinfrastrukturen in Deutschland Gegenstand gezielter Anschläge werden" (BMI, 2005, p. 3).

[111] From the original in german: "(…) auch das aktive Einbringen deutscher Interessen in die politische Willensbildung auf internationaler Ebene." (BMI, 2005, p. 9).

[112] From the original in german: "Deshalb ist es für die Sicherheit der deutschen Informationsgesellschaft und für den Industriestandort Deutschland unabdingbar, dass zur Gewährleistung vertraulicher Kommunikation innovative, vertrauenswürdige Kryptoprodukte verfügbar sind (BMI, 2005, p.11).

vulnerable, "not least with a view to criminal activities, terrorist attacks or military attacks from or against cyberspace"(BMVg, 2006, p.19, own translation)[113].

Despite these acknowledgments, the 2006 White Paper did not enter further details about cyber issues. It was restricted to state, "These new types of risks cannot be countered either solely or primarily with military means" (BMVg, 2006, p. 19, own translation)[114]. Here, one can observe that despite mentioning military use, there is clear restrain from viewing cybersecurity solely as a military domain. Thus, Germany sought a more balanced view of IT security, mainly stressing a civilian focus.

Following the focus on infrastructure protection, in 2007, Germany launched the CIP Implementation Plan (*Umsetzungsplan Kritis*- UP-KRITIS). This Plan acknowledged that the growing dependencies of the private sector demanded an "adequate protection of information infrastructures in Germany -and worldwide" that could "no longer be achieved solely through IT security measures in companies and organizations" (BMI, 2007, p. 6, own translation)[115]. Therefore, UP-KRITIS explained that measures would be necessary at both the individual level of the organizations and companies themselves and in sectors "where the shares of critical infrastructures of different companies are closely intertwined or interdependent in order to increase reliability through coordinated measures" (BMI, 2007, p. 6, own translation)[116].

In this regard, UP-KRITIS was designed for critical infrastructure operators in cooperation with the federal government to “focus on preventative action and reaction to IT crises” (BSI, 2007, p. 55). To complement the UP-KRITIS efforts, in late 2007, UP-BUND (*Unsetzungsplan Bund*) was launched. It created a basis for IT security implementation for the Federal government’s administration to transform IT security in public administration “from a multitude of one-off activities into a continuous process that is to be maintained by qualified and authorized personnel” (BSI, 2009, p. 11).

Besides the two plans, a military approach was further on IT security. In the Strategic Reconnaissance Command, a unit to carry out computer network operations (CNO) was

[113] From the original in German: “Als Folge sind Deutschlands politische und wirtschaftliche Strukturen sowie seine kritische Infrastruktur verwundbarer geworden, nicht zuletzt mit Blick auf kriminelle Aktivitäten, terroristische Anschläge oder militärische Angriffe aus dem oder gegen den Cyber-Raum”(BMVg, 2006, p.19).

[114] From the original in German: “Allerdings kann diesen neuartigen Risiken weder allein noch vorrangig mit militärischen Mitteln begegnet werden” (BMVg, 2006, p.19).

[115] From the priginal in German: “Demzufolge kann ein angemessener Schutz der Informationsinfrastrukturen in Deutschland –und weltweit – nicht mehr allein durch IT-Sicherheitsmaßnahmen in den Unternehmen und Organisationen erreicht werden“ (BMI, 2007, p. 6).

[116] From the original in German: “wenn die Anteile Kritischer Infrastrukturen verschiedener Unternehmen eng miteinander verflochten beziehungsweise voneinander abhängig sind, um durch abgestimmte und koordinierte Maßnahmen die Verlässlichkeit zu erhöhen (BMI, 2007, p. 6).

founded. Its task involves working in enemy networks and, if necessary, accompanying conventional military measures (STEIGER, 2022). The Ministry of Defence (BMVg) explained that “As part of their mission, enemy abilities are analyzed to support forces of the German Armed Forces in the operational and crisis areas, but the effect in enemy computer networks is also simulated”[117] (DEUTSCHER BUNDESTAG, 2014, p.1165, own translation). In this regard, an idea of offensive capability development can be raised. Still, BMVg considered an independent, detached action in the sense of a "cyberwar" to be unlikely (STEIGER, 2022; DEUTSCHER BUNDESTAG, 2014).

The subtle movement toward developing offensive capabilities corroborates a restrained culture. As Steiger (2022, p. 364, own translation)[118] stresses, the Federal Government “advocated promoting international rules for self-restraint to create a “culture of restraint,” including specification of international agreements and the international community voluntary self-restraint. Moreover, “The Federal Government underlined its own reluctance, for example, by the fact that the Bundeswehr should not develop malware or that the armed forces should not carry out any cyber attacks against targets abroad” (STEIGER, 2022, p. 364, own translation)[119]. In this regard, Germany's digital mentality was vigorously marketed by a self-restraint element. This element can be interpreted as mirroring Germany’s civil and self-restraining strategic culture (BERGER 1998; DUFFIELD 1998; ERB 2003; RITTBERGER 2001; WEBBER, 2001).

The concern over IT security continued to grow. In 2008 the German Constitutional Court established a landmark ruling. The Court developed the doctrine of the government's responsibility to "guarantee the confidentiality and integrity of information technology systems" (BVERF, 2008). One year later, the CIP Strategy would be launched. The CIP Strategy stressed that "critical infrastructure protection is a task to be performed jointly by government, companies and/or operators and also by civil society," having two guiding principles regarding infrastructure protection: trusting cooperation between state, business, and industry; and the requirement of suitability, and proportionality on measures taken and the

[117] From the original in German: “Im Rahmen ihres Auftrages werden zur Unterstützung von Kräften der Bundeswehr in den Einsatz- und Krisengebieten gegnerische Fähigkeiten analysiert, aber auch das Wirken in gegnerischen Computernetzwerken simuliert”.

[118] From the priginal in German: Die Bundesregierung sah in einem durch militärische Feindseligkeit geprägten Cyberspace aber auch ein erhebliches Risiko und plädierte dafür, internationale Regeln zur Selbstbeschränkung zu fördern, um eine »Kultur der Zurückhaltung zu schaffen« (STEIGER, 2022, p. 364).

[119] From the original in German: Die Bundesregierung unterstrich die eigene Zurückhaltung bspw. dadurch, dass die Bundeswehr keine Schadsoftware entwickeln sollte bzw. dass die Streitkräfte keine Cyberangriffe gegen Ziele im Ausland durchführten „ (STEIGER, 2022, p. 364).

use of resources made for increasing protection level (BMI, 2009, p. 12). In this regard, even if narrow to critical infrastructure protection, a whole of society narrative was being designed.

The technical focus of the subject has not entirely separated the political and diplomatic discussions on the subject in Germany. To be an active player in international decision-making discussions, the country has participated, for instance, since 2004, in the United Nations Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security (UNGGE). In this sense, the country has participated in all six Groups of Governmental Experts (GGE) that have "studied the threats posed by the use of ICTs in the context of international security and how these threats should be addressed" (UN, 2022), a relevant fact as it is not a P5 country[120]. However, more concretely, only after the Estonia cyber attacks in 2007, the Georgia hybrid conflict in 2008, and the repercussion of malware Stuxnet in Iran in 2010 did BMI start to be more involved and pay closer attention to cyberspace. This led to the development of Germany's first National Cybersecurity Strategy (NCSS) in 2011.

The 2011 NCSS was the first German document to use the term cyberspace. It described cyberspace as:

> […] the virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace (FEDERAL MINISTRY OF INTERIOR, 2011, p. 14).

In this regard, one can infer that Germans understand cyberspace as a broader concept than IT security. Besides, the strategy makes a threat assessment acknowledging criminals, terrorists, and spies as actors using cyberspace for their activities in a transnational manner.

The NCSS exposed that "Military operations can also be behind such attacks," emphasizing that the Stuxnet case showed that important industrial infrastructures are no longer exempted from targeted IT attacks (FEDERAL MINISTRY OF INTERIOR, 2011, p. 3). In this regard, the strategy clearly stated that cybersecurity would need a comprehensive approach. It would focus mainly on civilian approaches and measures, complemented by the Bundeswehr "to protect its capabilities and measures based on mandates to make cyber security a part of Germany's preventive security strategy" (FEDERAL MINISTRY OF INTERIOR, 2011, p. 5).

[120] P5 refers to the permanent members of the United Nations Security Council, which are: China, France, Russia, the United Kingdom, and the United States.

The strategy also exposed that given the "global nature of information and communications technologies," efforts at the domestic and international levels would need to be observed to generate coherence and protection capabilities. Thus "international coordination and appropriate networks focusing on foreign and security policy aspects" would be important, especially involving cooperation with the United Nations, EU, NATO, the G8[121], the OSCE, and other multinational organizations (FEDERAL MINISTRY OF INTERIOR, 2011, p. 5). In this sense, it calls attention to another cornerstone of Germany's strategic culture: multilateralism and a solid commitment to multilateral institutions (SIEDSCHLAG, 2007).

Amid this context, the NCSS sets ten strategic objectives:

a) Protection of critical information infrastructures
b) Secure IT systems in Germany
c) Strengthening IT security in the public administration
d) Set a National Cyber Response Center[122]
e) Set a National Cyber Security Council[123]
f) Effective crime control also in cyberspace
g) Effective coordinated action to ensure cyber security in Europe and worldwide
h) Use of reliable and trustworthy information technology
i) Personnel development in federal authorities
j) Tools to respond to cyber attacks (FEDERAL MINISTRY OF INTERIOR, 2011)

Among these objectives, when one observes cybersecurity elements, it calls attention to the placement of critical information infrastructure protection and the response to cyber attacks. This placement shows a defensive tone for the NCSS and a continuum concern over the physical integrity of infrastructures. Besides, stating under the tenth objective, "We will continue to assess the threat situation regularly and take appropriate protection measures" (FEDERAL MINISTRY OF INTERIOR, 2011. p. 12), the NCSS gave a loose interpretation of protective measures. The concern with critical infrastructure and, thus, data protection leads one to infer that Germany recognized conventional military and informational power aspects of the digital realm.

[121] G7 since 2014.

[122] Nationales Cyber-Abwehrzentrum (Cyber-AZ). Cyber-AZ is “tasked with optimizing operational cooperation between government agencies with regard to various hazards in cyberspace and for coordinating the appropriate protective and defensive measures” (BEIGEL; HERPIG, 2021, p. 81).

[123] Nationaler Cyber-Sicherheitsrat (Cyber-SR). “As a strategic advisor to the Federal Government, the Cyber-SR aims to identify requirements for long-term action as well as trends in cybersecurity to stimulate appropriate impulses” (BEIGEL; HERPIG, 2021, p. 80).

Also, in the explanation of the eighth objective, the strategy set Germany's intention to strengthen the "technological sovereignty and economic capacity" of the country "in the entire range of core strategic IT competencies, include them in our political strategies, and develop them further" (FEDERAL MINISTRY OF INTERIOR, 2011, p. 11). This element exposes the perception of the economic power of digital dynamics.

In addition, the strategy is called under the seventh objective to push forward national interests and ideas related to cyber security in multilateral forums. In this sense, it explains the need for the establishment of a "code for state conduct in cyberspace (cyber code)" among countries, including confidence-building security measures (FEDERAL MINISTRY OF INTERIOR, 2011, p. 11). These elements demonstrate awareness of what one would classify as political and diplomatic powers conventionally.

Building on the first German Cybersecurity Strategy, one can infer that the country was still building itself domestically. Despite mentioning the need for a broad international cooperation effort, a heavier focus on building proper institutions to deal with the digital world and its interface with the physical one (especially on critical infrastructure protection) appeared. Moreover, the strategy did not suggest any assertive response to prevent cyber attacks. In this regard, and given the loose text, Germany's self-perception was poorly defined. However, the reference to strengthening its economy and pushing an international normative debate can be interpreted as the country seeing itself as a technological sovereign country with an international coordination role of cybersecurity efforts and standards development.

It is also important to note that the NCSS followed the techno-civilian approach of previous strategic documents, even mentioning cyberspace as a broader concept and acknowledging several spheres of action (diplomatic, economic, military, political, and informational). Some goals were still directed to IT security. Notwithstanding, the technical perception would be less present in further strategic documents. One example was the BMVg’s Defense Policy (*Verteidigungspolitische Richtlinien*), in which it was acknowledged that “With the threat from the information space, states will adapt their previous ideas about conflicts and their possible solutions” (BMVg, 2011, p. 9, own translation)[124].

The multilateral character of Germany's strategic culture would also be present in the 2011 Defense Policy since the document exposed the significant increase in vulnerability of national security systems to cyber attacks that required effective and coordinated responses within NATO. The document explained the necessity to have capabilities to defend against

[124] From the original from German: “Mit der Bedrohung aus dem Informationsraum werden Staaten ihre bisherigen Vorstellungen über Konflikte und ihre Lösungsmöglichkeiten anpassen” (BMVg, 2011, p. 9).

cyber attacks, expanding the alliance's range of tasks and reinforcing that the “common defense under Article 5 of the NATO Treaty remains at the core of the Alliance” (BMVg, 2011, p. 17, own translation)[125]. In this sense, Germany advocated internationally "that cyber-attacks within NATO should not be automatically treated under Article 5"(STEIGER, 2022, p. 367, own translation) and that fighting cyber threats was primarily a matter for civilian institutions (DEUTSCHER BUNDESTAG, 2010, p. 8097)[126]. Thus, a civilian approach to cyber threats was reinforced.

Germany would remain focused on its domestic cyber security development in the following years. As Steiger (2022, p.368, own translation)[127] highlights, by taking the view that “the development and use of malware by the Bundeswehr did not represent a fundamental legal problem," offensive capabilities would have been developed. In this regard, in 2012, Germany revealed the capacity to conduct offensive cyber operations (DPA, 2012). Also, the 2011-2013 report of the Parliamentary Control Body that oversees German intelligence services (*Parlamentarische Kontrollgremium* – PKGr)[128] included discussions over cyber threats. It pointed out that "the importance of national security in the IT sector should not be underestimated in the future and that greater efforts to protect against cyber threats would be required both in the state and in the private sector" (DEUTSCHER BUNDESTAG, 2013, p. 9-10, own translation)[129]. Thus, one can infer that cybersecurity was gaining a crescent relevance in Germany's agenda. Despite the political ascendency, the topic's relevance would remain with a technical approach, especially considering the developments after the Snowden revelations in 2013.

The Snowden revelations showed that Germany was being spied on by the United States of America's National Security Agency (NSA), including the cell phone of Chancellor Angela Merkel. In this regard, the relationship between Germany and the USA was scrutinized. Germany sent a catalog of questions to the US government on 11 June, 26 August,

[125] From the original in German: “Die gemeinsame Verteidigung gemäß Artikel 5 des NATOVertrages bleibt der Kern des Bündnisses” (BMVg, 2011, p. 17).

[126] From the original in German: “Cyberangriffen innerhalb der NATO nicht automatisch nach Artikel 5 zu behandeln” (STEIGER, 2022, p. 367).

[127] From the original in German: “dass der Aufbau und Einsatz von Schadesoftware durch die Bundeswehrkein gründsätzliches rechtliches Probleme darstelle” (STEIGER, 2022, p. 368).

[128] "The Parliamentary Control Committee (PKGr) is responsible for controlling the federal intelligence services and monitors the Federal Intelligence Service (BND), the Military Counterintelligence Service (MAD), and the Federal Office for the Protection of the Constitution (BfV)" (DEUTSCHER BUNDESTAG, 2022a, own translation).

[129] From the original in German: Es kam dabei zu dem Ergebnis, dass künftig die Bedeutung der nationalen Sicherheit im IT-Bereich nicht unterschätzt werden dürfe und größere Anstrengungen zum Schutz gegen Cyberbedrohungen sowohl im staatlichen als auch im privatwirtschaftlichen Bereich erforderlich seien (DEUTSCHER BUNDESTAG, 2013, p. 9-10).

and 24 October 2013. Besides, during a visit to NSA headquarters at the beginning of November, the heads of the Federal Intelligence Service (*Bundesnachrichtendienst* – BND) and the Domestic Intelligence Service (*Bundesamt für Verfassungsschutz* -BfV) asked the most important questions in person, handing over a written list. However, no answers were delivered (SPIEGEL, 2014).

The revelations triggered a dual movement from Germany: at the domestic and international levels. At the domestic level, the country sought to evaluate how the intelligence services of the partner states had undermined it. Thus, the BSI and BMI investigated service providers who had contracts with the Federal government to evaluate the extent to which these foreign intelligence services had become the target of the surveillance measures or made data available. At the same time, there was a physical check to determine where access to lines could be taken (STEIGER, 2022).

At the international level, Germany sought a normative approach to "change the disclosed practices and to encourage more restraint from states in regards to spying" (STEIGER, 2022, p. 253, own translation)[130]. In this regard, while falling short of establishing bilateral agreements to limit espionage, Germany, along with Brazil, spearheaded the UN draft resolution condemning surveillance, which resulted in the UN General Assembly Resolution 68/167 entitled 'The Right to Privacy in the Digital Age' (JOYCE, 2015).

In 2014 a parliamentary inquiry committee was set to investigate the NSA's data collection practices and the German intelligence agencies' cooperation with the NSA and other "Five Eye Alliance" intelligence services. The committee found that BND had closely collaborated with the NSA in monitoring international telecommunications on German territory, thus engaging in illegal practices according to German legislation (SCHALLBRUCH; SKIERKA, 2018). The committee's result led the Federal Government to admit that "there had apparently been shortcomings in the cooperation between the BND and the NSA." However, no confrontation was set since Germany's security depended on the USA partnership (STEIGER, 2022, p. 298, own translation)[131].

Despite not moving forward with a more assertive agenda toward the USA, the Snowden revelations caused a serious discussion related to the technological sovereignty of Germany. According to Schallbruch and Skierka (2018, p. 10).

[130] From the original in German: "die enthüllten Praktiken zu verändern und für mehr staatliche Zuruckshältung zu werben" (STEIGER, 2022, p. 253).

[131] From the original in German:"dass es offenbar Missstände bei der Kooperation zwischen BND und NSA gegeben habe".

> Never before and never since has a coalition agreement to form a German government included such a comprehensive agenda on cybersecurity. The government coalition parties agreed on the adoption of an IT security law, as well as on the strengthening of the Federal Office for Information Security's (BSI) role in cybersecurity. For the first time, Germany's coalition agreement also calls for "regaining Germany's technological sovereignty."The idea behind this call for action was to introduce technical, legal, and political measures to better protect citizens, industry, and state authorities from surveillance by foreign intelligence agencies.

Germany would have a more assertive position to safeguard its strategic surroundings (Europe), accelerating discussions over European data protection legislation and encompassing standards for data transfer to the USA and non-EU states (SCHALLBRUCH; SKIERKA, 2018).

The concrete debate over technological sovereignty was similar to France's position. The idea to strengthen the IT security industry was put in place to diminish USA dependencies. From its beginning, the Digital Agenda 2014-2017 stressed Germany's more assertive position to become a "global leader in the area of market penetration and use of digital services" (THE FEDERAL GOVERNMENT, 2014, p. 9).

Besides, the document exposed Germany’s efforts to:

a) Strengthen BSI's role (which would include the deployment of more resources);

b) Increase the coordinating role of the National Cyber Response Center (*Nationalen Cyber-Abwehrzent);*

c) Expand the Cyber Crime Center in the Federal Criminal Police Office (*Bundeskriminalamt* – BKA);

d) Reinforce measures, tools, and expertise within the Federal Office for the Protection of the Constitution;

e) Work internationally with the European Network and Information Security Agency and Europol‘s European Cybercrime Centre;

f) Adapt criminal law, considering the loopholes related to handling stolen data.

Worth noticing as well is that the Digital Agenda 2014-2017 emphasizes, under the agenda's integration in the international context, the continuation of the transatlantic dialogue as " an example of a stronger multistakeholder focus” and that Germany was in favor of a "peaceful alignment of international cybersecurity policy," rather than a cyber arms race (THE FEDERAL GOVERNMENT, 2014, p. 35). These elements preserve Germany’s multistakeholder and normative approach to cybersecurity in the international sphere.

Still, “The State of IT Security in Germany 2014” indicated a more assertive approach to intelligence agencies. The document exposed, "The primary purpose of cyber attacks by government intelligence agencies is military and economic espionage. "It also affirmed that the military sector cyberspace has today become a further key domain alongside the classical military domains and indicated that “Given their quality, defending against these attacks is only possible by putting a great deal of effort and money into countermeasures” (BSI, 2014, p. 24). PKGr exposed a similar approach in its 2013-2015 report. The document stated, "It became clear that the German intelligence services have to be further developed technically and in terms of personnel so that the increasing cyber threats can be countered effectively" (DEUTSCHER BUNDESTAG, 2016, p. 10, own translation)[132].

The IT Security Act (*Gesetz zur Erhöhung der Sicherheit Informationstechnischer Systeme* -IT-SiG), previously discussed in 2013, entered into force in 2015, amending past laws such as the German Telemedia Act of 2003 and the Federal Data Protection Act (ROMANIUK; CLAUS, 2021). It was designed to require critical infrastructure operators to have minimum IT security levels and prove they were implementing them. Besides, its Section 5 and through the future message rates from essential companies of infrastructure as defined by Section 8b, the BSI would again expand its capabilities. This would allow the agency to "make an improved statement on current cyber-security, including in relation to intelligence attacks in German cyber-space" (BSI, 2015, p. 35).

Notwithstanding, 2015 would mark Germany's digital mentality again, triggering a change in the country's cybersecurity approach. The Bundestag Hack, a moderated successful cyber operation against the German Federal Parliament, widely exposed the vulnerabilities of German agencies. According to a Greens politician, Steffi Lemke, the attack revealed that "the Interior Ministry has completely missed out on establishing a functioning cyber defense" (DW, 2015). In this regard, Germany started to add a military component to its cybersecurity reasoning, adding it to a "technically-oriented cybersecurity policy focusing on data protection aspects and preventive technology management" (SCHALLBRUCH; SKIERKA, 2018, p. 12). Besides, discussions on active cyber defense (mainly transvestite as hack-back debates) emerged.

The change from a techno-civilian approach to a civilian-military approach, more encompassing, transformed Germany’s digital mentality into a truly global approach. The first signals of the shift were set with the development by the BMVg of strategic guidelines for cyber defense. The document, disclosed in full by Netzpolitik (2015), explained that it

[132] From the original in German: “Deutlich wurde, dass die deutschen Nachrichtendienste technisch und personell so weiterentwickelt werden müssen, dass den zunehmenden Cyberbedrohungen wirksam begegnet werden kann” (DEUTSCHER BUNDESTAG, 2016, p. 10).

expanded the definition of cyberspace set in the NCSS to include the “proportion of IT systems that have data interfaces but are otherwise separated from publicly accessible networks and the Internet.” (NETZPOLITIK, 2015, own translation)[133].

In this regard, the strategy affirmed that cyberspace would be another organizational area (*Organisationsbereich*), such as air, land, sea, and space. It also highlighted five fields of action, including the contribution to national security precautions, shaping international framework conditions, and risk mitigation. Moreover, the document pointed out that the offensive cyber capabilities of the Bundeswehr were to be seen as "supporting, complementary or substitutive means of action" (NETZPOLITIK, 2015, own translation)[134].

If Germany’s approach change started with the BMVg's Strategy, one could affirm it was consolidated in the 2016 White Paper and Germany’s second NCSS.

5.1.2 The second phase (2016-2021): Global approach

Since it took ten years to reach the update on Germany's White Paper, it encompassed cybersecurity more profoundly. The document acknowledged the need for defensive and offensive capabilities to secure cyberspace, including a cyber reserve. In this regard, it clearly stated the need for a whole-of-government endeavor toward cyber security. It considered that criminals, individuals, or terrorists could cause great damage to society and that the threat landscape would encompass a broad spectrum of activities. These include theft and fraudulent use of personal data, industrial espionage, damage to critical infrastructure, and the disruption or complete shutdown of government and military communications (THE FEDERAL GOVERNMENT, 2016).

According to the document:

> Ensuring cyber security and defence is therefore a whole-of-government task that must be performed collectively. This includes the joint protection of critical infrastructure. The tasks to be carried out are specified in the Cyber Security Strategy, which is developed under the direction of the Federal Ministry of the Interior. Defense aspects of whole-of-government cyber security are core tasks of the Federal Ministry of Defence and the Bundeswehr, while overall responsibility for international cyber security policy lies with the Federal Foreign Office (THE FEDERAL GOVERNMENT, 2016, p. 38).

[133] From the original in German: “Diese Strategische Leitlinie erweitert diese Definition um den Anteil der IT-Systeme, die über Datenschnittstellen verfügen, ansonsten aber von öffentlich zugänglichen Netzen und dem Internet separiert sind“ (NETZPOLITIK, 2015).

[134] From the original in German: “Offensive Cyber-Fähigkeiten der Bundeswehr sind als unterstützendes, komplementäres oder substituierendes Wirkmittel anzusehen” (NETZPOLITIK, 2015).

In this regard, although adding the military component to its approach, Germany tried to make a sometimes blurred separation between security and defense agencies. It also reinforced the importance of public-private partnerships for the protection of the economy. The element of strengthening industry at the national and European levels appears again. When the White paper puts that "Europe needs a strong and competitive defence industry of its own if it is to assume joint responsibility for security" (THE FEDERAL GOVERNMENT, 2016, p. 74). Also when it says that "Germany's competitiveness as an industrial nation therefore depends all the more on maintaining its lead in innovation" (THE FEDERAL GOVERNMENT, 2016, p. 22).

Another relevant point set by the White Paper was the parallel between cyber-attacks and armed attacks and the tendency to increase operations in the cyber and information domain in military conflict (THE FEDERAL GOVERNMENT, 2016, p. 36). The document highlighted that attempts to establish internationally binding regulations or confidence- and security-building measures could have a limited effect (THE FEDERAL GOVERNMENT, 2016, p. 37). Notwithstanding, Germany would work to: reach a common understanding of international law applicability to the cyber and information domain, establish confidence-building measures and transparency on the cyber security policy of participating States of the OSCE, and develop guidelines for states' behavior conduct code in cyberspace (THE FEDERAL GOVERNMENT, 2016, p. 82). The White Paper, thus, complemented the second NCSS.

The second German NCSS stated in its guidelines that "Germany must maintain its sovereignty and ability to function even in the digital age" (BMI, 2016, p. 8, own translation)[135]. In this sense, it acknowledged that attackers "often have a criminal, extremist/terrorist, military or intelligence background" and that "Political and military conflicts are often accompanied by cyber campaigns or are waged in cyberspace below the threshold of armed conflict," which makes political assessments, and thus countermeasures, more complex (BMI, 2016, p.7, own translation)[136].

Besides, the document stated that challenges posed by cyberspace would imply a shared responsibility between the government, private industry, society, and the research community to secure the digital realm. Moreover, it posed that "Close European and

[135] From the original in German: Die Handlungsfähigkeit und Souveränität Deutschlands müssen auch im Zeitalter der Digitalisierung gewährleistet sein" (BMI, 2016, p. 8).

[136] From the original in German: Die Angreifer haben vielfach einen kriminellen, extremistischen/terroristischen, militärischen oder nachrichtendienstlichen Hintergrund (…) Politisch-militärische Konflikte werden oft von Cyber-Kampagnen begleitet oder unterhalb der Schwelle zum bewaffneten Konflikt auch im Cyber-Raum ausgetragen (BMI, 2016, p.7).

international coordination is particularly important due to often cross-border interdependencies and threats indispensable from a foreign and security policy point of view" (BMI, 2016, p. 9, own translation)[137]. Amid this context, the NCSS set priority in four action areas:

a) Safe and Self-determined Action in a Digitized Environment
b) A Joint Effort of Government and Industry
c) An Effective and Sustainable Cybersecurity Architecture
d) The Active Positioning of Germany in European and International Cybersecurity Policy Discussions (BMI, 2016).

The first priority area recalled the idea of digital autonomy. Thus, it targeted IT security research and development, certification policy, support for secure electronic identities, and encryption of electronic communications and services offered via the Internet. In this regard, it calls attention to the ideas of “security through encryption "and security despite encryption." Thus, while users should have their data protected by encryption, law enforcement and security authorities could fall under "strict legal conditions" to decrypt/bypass encrypted communications if necessary to carry out their duties as required by law. Besides, the strategy emphasizes the need to strengthen centers of excellence in IT security (CRISP in Darmstadt, CISPA in Saarbrücken; KASTEL in Karlsruhe) and cyber defense (Cyber Defence and Smart Data research centre of the Bundeswehr University in Munich). These elements represent a parallel to the idea of conventional informational power.

The second priority area focused on the need for public-private partnerships and Germany to have a strong IT industry. In this regard, besides the concern on critical infrastructure protection, it calls attention to the explicit will from the Federal government to promote the quality label "IT Security Made in Germany" and expand the existing foreign trade instruments. These elements resonate with the 204 -2017 Digital Agenda, significantly deepening Germany's perception of autonomy through solid national industry and its aim to be a 4.0 industrial leader. Here the economic power of cyberspace is present.

The third priority area focused on the government's role in ensuring security, law, and freedom and the capacity of governmental institutions to protect citizens and themselves. The NCSS stated: "The scope of tasks is broad and ranges -in compliance with constitutional limits -from prevention, averting danger and criminal prosecution to counter-espionage and

[137]From the original in German: “Eine enge europäische und internationale Abstimmung ist dabei insbesondere aufgrund oftmals grenzüberschreitender Interdependenzen und Bedrohungen unter außen- und sicherheitspolitischen Gesichtspunkten unverzichtbar.” (BMI, 2016, p. 9).

intelligence to cyber defense" (BMI, 2016, 27, own translation)[138]. In this regard, the proposals, in general, were about further developing response capabilities (including BKA, BSI, BfV, and the military remit), intensifying law enforcement in cyberspace, improving human resources, and increasing coordination within the German federalism system (Federal Government and Länder).

This action area calls attention to a further institutional effort with the creation of the Central Office for Information Technology in the Security Sector (*Zentralen Stelle für Informationstechnik im Sicherheitsbereich* – ZITiS). The center was designed to support authorities' operational cyber capabilities, including counterintelligence and taking advantage of possible synergies, and was inaugurated in 2017. Moreover, the NCSS explained, "In accordance with its legal mandate, the BND records cyber espionage and other cyber attacks against state and/or critical infrastructures in Germany abroad" (BMI, 2016, p. 32, own translation)[139.] Thus, in 2016 the relevance of a controversial law that expanded the agency's surveillance powers (*BND Gesetz*) (SCHALLBRUCH; SKIERKA, 2018). With these movements, one can infer a parallel with ideas of conventional military power present in the 2016 NCSS.

The fourth area of action demonstrates the willingness to use diplomatic channels to achieve cybersecurity, and thus the parallel with conventional diplomatic power. The strategy mentioned that when dealing with cyber-attacks using foreign systems, "the use of diplomatic channels should also be regularly considered in addition to measures to protect and restore the compromised systems and to prosecute the perpetrators" (BMI, 2016, p. 39, own translation)[140].

Besides, the action area explains Germany's aim to push for: cyber security architectures and standards (at the European level), strengthen law international enforcement, foster bilateral and regional support cooperation for cyber capacity building, and campaigns for greater cyber security in the relevant forums such as NATO, Organization for Security and Co-operation in Europe (OSCE) and UN. In this regard, Germany assumed the rotating

[138] From the original in German: "Das Aufgabenfeld ist breit und reicht – unter Beachtung der verfassungsrechtlich gebotenen Grenzen – von der Prävention, der Gefahrenabwehr und der Strafverfolgung über die Spionageabwehr und nachrichtendienstliche Aufklärung bis zur Cyber-Verteidigung (BMI, 2016, p. 27).

[139]From the original in German: "Der BND erfasst gemäß seinem gesetzlichen Auftrag im Ausland Cyber-Spionage- und sonstige Cyber-Angriffe, die sich gegen staatliche und/oder Kritische Infrastrukturen in Deutschland richten" (BMI, 2016, p. 32).

[140] From the original in German: "(…) sind regelmäßig auch die Nutzung diplomatischer Kanäle neben Maßnahmen zum Schutz und zur Wiederherstellung der beeinträchtigten Systeme und zur Verfolgung der Täter in Erwägung zu ziehen" (BMI, 2016, p. 39).

position in OSCE in 2016. Under Germany's mandate within the organization, OSCE passed a series of Confidence Building Measures, including efforts to improve regional collaboration, critical infrastructure protection, crisis communication channels, and public-private partnerships (ROMANIUK; CLAUS, 2021).

Adopting a global (civil-military) approach led Germany to further developments within the military realm. In 2016, the division 'Cyber- and Information technology' (*Abteilung Cyber- und Informationstechnik*, CIT) in BMVg, possessed two subdivisions: CIT I (Methods and Digitalisation) and CIT II: (Capabilities Cyber/IT). One year later, following ministerial recommendation, the Cyber and Information Domain Service (*Cyber- und Informationsraum*, CIR) was structured around the Cyber and Information Domain Command (*Kommando Cyber- und Informationsraum*, KdoCIR) (CYMUTTA, 2020).

KdoCIR follows a comprehensive approach, combining “all forces needed for the reconnaissance, operation, and management of cyberspace in one military organisational area” (SCHALLBRUCH; SKIERKA, 2018, p. 37). In this sense, it is supported by three sub-organizations: Strategic Reconnaissance Command (*Kommando Strategische Aufklärung*, KSA), Bundeswehr Geoinformation Centre (*Zentrum für Geoinformationswesen der Bundeswehr*, ZgeoBw), and the Information Technology Command (*Kommando Informationstechnik der Bundeswehr*, KdoITBw) (CYMUTTA, 2020).

In 2016 Germany would also be more engaged within NATO. It signed NATO’s Cyber Defence Pledge committing itself to “constantly increasing its national resilience in cyber security to play its part in the Alliance’s defence capability” (BSI, 2018, p. 86). Besides, the 2011 Memorandum of Understanding (MoU) with the organization was confirmed in 2016. The BSI has been appointed Germany's National Cyber Defence Authority (NCDA) (BSI, 2018).

Additionally, major cyber events contributed to the deepening of Germany's perception of the need to possess reactions and repression capabilities. In the 2017 "The State of IT Security in Germany" report, BSI stated that "Germany must be prepared for this scenario [cyber attacks on the Bundestag election] – also against the backdrop of the cyber attacks that have taken place in the US and France" (BSI, 2017, p. 17). Besides, the Wannacry and NotPetya ransomware attacks in 2017 impacted the country.

According to Der Spiegel (2017), Deutsche Bahn computers were caught in the Wannacry attack, affecting digital display boards, ticket machines, and video surveillance technology. Regarding NotPetya, several German companies were affected (BSI, 2017). The range of cyber attacks led the PKGr to affirm that “it became clear that the capabilities of the

German intelligence services must be further expanded in terms of technology and personnel to be able to effectively investigate cyber threats" (DEUTSCHER BUNDESTAG, 2018, p. 11 own translation)[141] . In this regard, the inauguration of ZITiS in 2017 becomes relevant. This is so since its supportive role is directed to "digital forensics, telecommunications surveillance, crypto, and big-data analysis. ZITiS also works on technical questions related to the fight against crime, as well as in emergency response and counterintelligence" (BEIGEL; HERPIG, 2021, p. 84-85).

In 2018 BSI highlighted that even though no significant waves of ransomware emerged, "ransomware must continue to be classified as a massive threat" (BSI, 2018, p. 91). Besides, its IT security report showed that methods of mass distribution of malware had been further developed and that illegal crypto-mining was added as a relevant threat. In this regard, BSI pointed out that Germany's threat landscape became more complex, increasing protection costs.

Also, in 2018, the Strategic Reconnaissance Command was founded. The new agency had the task of including satellite-based imaging reconnaissance, communications and electronic reconnaissance, electronic warfare, and the area of object analysis (STEIGER, 2022; BUNDESWEHR, 2022). Moreover, BMI and BMVg, in cooperation, decided to found the Agency for Innovation in Cyber Security (Cyber-Agentur), which is a "joint civil-military DARPA-like agency to foster cybersecurity and cyber defense research" (HERPIG, MORGUS; SHENIAK, 2020, p. 4). The formation process of the agency was completed in August 2020, and the first commissions were made by the end of 2020. The agency works to coordinate the needs of security agencies and improves cooperation between federal authorities, academia, and the private sector and had a budget allocation of 200 million euros from 2019 to 2022 (BEIGEL; HERPIG, 2021; REINHOLD; REUTER, 2019).

In 2019 another relevant effort was made: the National Cybersecurity Pact (*Nationaler Pakt Cybersicherheit*). This Pact is a BMI initiative intended to support the Paris Call for Trust and Security in Cyberspace as a German contribution. In this sense, the pact was designed to apply a whole-of-a-society approach, as it "involves all relevant groups, manufacturers, providers and users in society, as well as the public administration, in a national pact that reflects the shared responsibility for digital security" (BEIGEL; HERPIG, 2021, p. 81). As a first step, in 2020, the National Cybersecurity Pact identified and compiled

[141] From the original in German: "Deutlich wurde, dass die Fähigkeiten der deutschen Nachrichtendienste technisch und personell weiter ausgebaut werden müssen, um den Cyberbedrohungen wirksam aufklären zu können (DEUTSCHER BUNDESTAG, 2018, p.11).

the actors working in the cyber field and information security in a structured overall picture of cybersecurity activities in Germany (BMI, 2020).

Besides, the BSI’s remit was expanded to include issues such as “5G networking infrastructure, artificial intelligence, Digital Consumer Protection, a wider scope for consulting services provided to municipal and state actors, and the BSI as a central certification and standarisation body" (BSI, 2019, p. 4). This expansion resulted from the COVID-19 pandemic, which impacted Germany's digital mentality.

In 2020 BSI threat assessment included malware for mass cybercriminal attacks, data leaks, and critical vulnerabilities in software and hardware products. An entire section of "The State of IT Security in Germany" was dedicated to the "Threat to Cyber Security from the COVID-19 Pandemic", highlighting issues such as the social engineering attacks exploiting the pandemic situation and the increase of attack surface with the digitization jump derived from the social distancing and lock-down (BSI, 2020). Besides, on the overall threat assessment, BSI pointed to the emergence of new Advanced Persistent Threats (APT)[142]collectives which would be intended to pursue “tactical and strategic goals such as espionage or sabotage” (BSI, 2020, p. 35).

In this regard, it calls attention to the implementation for the first time of cyber sanctions by the EU in 2020, a process that Germany helped to initiate after the 2015 Bundestag Hack. On 30 July 2020, the EU imposed a travel ban and asset freeze against six individuals and three entities involved in various cyber attacks, including the cyber-attack against the Organization for the Prohibition of Chemical Weapons and those publicly known as 'WannaCry,' 'NotPetya,' and 'Operation Cloud Hopper' (COUNCIL OF THE EU, 2020). Later, in October 2020, the EU also sanctioned two Russian military officers over the 2015 Bundestag Hack (TIDEY, 2020). In this context, Germany's element of restraint was still present as the country “has been slow to publicly condemn the perpetrators’ (BENDIEK and SCHULZE, 2021), preferring to act within the scope of the EU for the sanctions applications. Notwithstanding, in 2022, the Federal Government started implementing an attribution process, a central issue related to the idea of a cyber sanctions regime. According to the document:

[142]“An APT denotes an intruder that can establish a persistence presence in a target network from which data can be constantly extracted and exfiltrated; leveraging a persistent presence also allows a disruptive or corruptive attack to be launched" (LIBICKI, 2021, p. 10). Due to the technical skills required for an APT to be put in place, they are usually linked to state or state-sponsored actors.

> To defend the international legal order in cyberspace, the Federal Government established a national attribution procedure for the first time in 2021, which regulates the attribution of responsibility for significant cyber attacks of international origin with the participation of all relevant specialist departments and coordinated by the Federal Foreign Office. In 2021, the results of the attribution process were included in the EU's public statements on the Russian-controlled SolarWinds hack, the China-related cyber attacks (statement of 19 July 2021 on the cyber actors APT 31, APT 40, and the Microsoft Exchange incident), and the "Ghostwriter" hack and disinformation campaign originating from Russia on 24 September 2021 (also a national declaration of attribution on 6 September 2021) (DEUTSCHER BUNDESTAG, 2022b, p. 84, own translation)[143].

A subtle shift toward a more assertive posture can be seen in this regard. This shift can also be backed by two critical developments throughout 2021: the IT Security Act 2.0 and the current National Cybersecurity strategy.

The IT Security Act 2.0 (*IT-Sicherheitsgesetz 2.0* – IT-SiG 2.0) strengthened BSI's competencies. It introduced new regulations for critical infrastructure operators, for the use of "critical components," and the new category of "companies of special public interest." According to the act, critical components would be the ones used in critical infrastructures and for which disruptions to availability, integrity, authenticity, and confidentiality "could lead to a failure or a significant impairment of the functioning of infrastructure or threats to public safety" (BUNDESGESETZBLATT TEIL I Nr. 25, 2021, p.1122, own translation)[144]. A the same time, "companies of special public interest" would include companies outside the classification of operators of critical infrastructures, thus including companies of relevant economic importance for the country or even as relevant suppliers "because of their unique selling points" (BUNDESGESETZBLATT TEIL I Nr. 25, 2021, p. 1123, own translation)[145]. In this regard, one can infer that the legislature considered the protection of supply chains as a relevant new component of cyber security.

[143] From the original in German: "Zur Verteidigung der internationalen Rechtsordnung im Cyberraum hat die Bundesregierung 2021 erstmals ein nationales Attribuierungsverfahren festgelegt, das unter Beteiligung aller relevanten Fachressorts und koordiniert durch das Auswärtigen Amt die Zuschreibung der Verantwortung für erhebliche Cyberattacken internationalen Ursprungs regelt. Ergebnisse der Attribuierungsverfahren fanden 2021 unter anderem Eingang in die öffentlichen Erklärungen der EU zum von Russland gesteuerten SolarWinds-Hack, den Cyberangriffen mit China-Bezug (Erklärung vom 19.07.2021 zu den Cyberakteuren APT 31, APT 40 und dem Microsoft Exchange-Vorfall) und der von Russland ausgehenden Hack- und Desinformationskampagne „Ghostwriter" am 24.09.2021 (hierzu auch nationale Attribuierungserklärung am 06.09.2021)" (DEUTSCHER BUNDESTAG, 2022b, p. 84).

[144] From the original in German: zu einem Ausfall oder zu einem erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen oder zu Gefährdungen für die öffentlichen Sicherheit führen können (BUNDESGESETZBLATT TEIL I Nr. 25, 2021, p. 1122).

[145] From the original in German: "(…) oder die für solche Unternehmen als Zulieferer wegen ihrer Alleinstelungsmerkmale von wessenlicher Bedeutung sind" (BUNDESGESETZBLATT TEIL I Nr. 25, 2021, p. 1123).

Along with major cyber attacks directed toward supply chains that gained international media highlights, such as SolarWinds[146] and Colonial Pipeline[147] , BSI cyber threat landscape assessment included attacks targeting healthcare organizations and critical vulnerabilities in Microsoft Exchange[148]. Moreover, the agency highlighted that cyber extortion attempts were becoming "the number one threat" and that vulnerabilities remained "one of the greatest challenges" for cybersecurity (BSI, 2021, p. 87).

The growing concern about cybersecurity and adopting a global approach in Germany's digital mentality can also be seen in the amount of financial support given to BSI over the years. According to the data provided by the *Haushaltsrechnung des Bundes*, the projected amount of money destined for BSI (Gesamtausgaben – Soll €) in 2011 was €69.036.000,00, while in 2016, this number increased to €88.706.000,00 (BMF, 2011; 2016). This configured a budget increase of 28% in a five-year time frame. Notwithstanding the rise in BSI's investment between the publication of the two previous NCSSs, the 2021 BSI's budget was set at 197,16 million Euros (BSI, 2022c), marking a further consolidation step toward Germany's global approach and a more assertive, more even if subtle, *modus operandi*.

The 2021 NCSS set out four crosscutting guiding principles:

a) Establishing cyber security is a joint task for the government, private industry, the research community, and society.

b) Reinforcing the digital sovereignty of the government, private industry, the research community, and society.

c) Making digital transformation secure.

d) Setting measurable, transparent objectives.

[146] "The SolarWinds hack is the commonly used term to refer to the supply chain breach that involved the SolarWinds Orion system. In this hack, suspected nation-state hackers that have been identified as a group known as Nobelium by Microsoft -- and often simply referred to as the SolarWinds Hackers by other researchers – gained access to the networks, systems and data of thousands of SolarWinds customers. The breadth of the hack is unprecedented and one of the largest, if not the largest, of its kind ever recorded" (OLADIMEJI; KERNER, 2021).

[147] "On 7 May 2021, the US pipeline operator Colonial Pipeline Company became aware of a cyber attack on its IT infrastructure. The following day, the affected operator reported the cyber attack as a confirmed ransomware deployment to the Federal Bureau of Investigation (FBI), the United States Department of Energy (DOE) and the White House. The attack affected the company's administrative network" (BSI, 2021, p. 17).

[148] "In March 2021, Microsoft published an unscheduled security update for its widely used groupware and e-mail server, Exchange. This patch closed four critical security holes, combinations of which had already been exploited in targeted attacks. One of these vulnerabilities allowed attackers to authenticate themselves to Exchange by sending it specially formatted HTTP requests. The other vulnerabilities could then be exploited to execute arbitrary program code and gain far-reaching access privileges. Attackers took advantage of these problems to plant backdoors on thousands of servers in the form of 'webshells. 'If these backdoors were not then removed after installation of the security update, perpetrators retained access to the affected systems and could use them to intercept mail or roll out malware, including ransomware variants. At the time the vulnerabilities were made public, some 98 percent of systems analysed in Germany were vulnerable. The first wave of exploits was mostly observed in cyber attacks conducted in the USA." (BSI, 2021, p. 27).

These principles would then detail four action areas with strategic objectives. The action areas are:

Remaining safe and autonomous in a digital environment

a) Government and private industry working together.
b) Strong and sustainable cyber security architecture for every level of government.
c) Providing high levels of cyber security in Germany is contingent on Germany’s active role in European and international cyber security policy (BMI, 2021).

In this regard, one can observe the continuation of a whole of society's approach to Germany's mentality. Besides, the idea of digital sovereignty appears more pronounced from the beginning of the strategy.

As for the main threat, the NCSS assessed cyber crime, cyber terrorism, cyber espionage, and cyber sabotage, emphasizing the perils of all these threats to critical infrastructure "in ways that can cause considerable financial and social impact" (BMI, 2021, p. 14). In this regard, it developed the threats within three categories: cybercrime, state-sponsored cyber attacks, and cyber attacks as components of hybrid threats. Interestingly, NCSS acknowledges the relevance of content manipulations (propaganda and disinformation) within hybrid threats. Still, the strategy stresses that its focus is not on "phishing crimes or threatening situations in which IT is used to disseminate illegal content. Instead, it focuses on cyber attacks that directly and substantially compromise IT systems' availability, integrity, and confidentiality" (BMI, 2021, p. 14).

Along with the threat assessment, the NCSS reinforces the perception of the relevance of a military component in security, as it acknowledges that military actors are developing capabilities. Therefore, the strategy explains, "This means that any assessment of the cyber threat situation must also take into account the military component” (BMI, 2021, p. 15). In this regard, one can observe the continuity of perception of conventional military power.

The conventional informational power perception can also be observed within the threat assessment. This is so since the NCSS acknowledges that cyberspace can impact the information domain and that disinformation and propaganda "can be particularly dangerous if they are disseminated as a result of cyber attacks on credible platforms" (BMI, 2021, p. 15).

Also, the NCSS pushes forward an economic element. By emphasizing that cyber attacks can affect prosperity, it builds upon the idea of conventional economic power. The document explains that "Germany's industry depends to a great extent on functional, reliable IT infrastructure of which the integrity is guaranteed," stressing that attacks on companies related to supply links and supply chains can have "massive financial consequences" (BMI, 2021, p. 16). Moreover, by acknowledging the need for "security by design" implementation as a default feature in "key enabling technologies" (IoT, AI, blockchain, big data, and quantum technology), the country indicates the focus areas for cooperation between industry and government (BMI, 2021. p. 49).

Besides these elements, when highlighting the concept of digital sovereignty, more emphasis is given to the economic relevance of cybersecurity. According to the strategy, Digital sovereignty is defined as "the capabilities and options of individuals and institutions to exercise their role(s) in the digital world independently, autonomously and safely" (BMI, 2021, p. 22). The independence and autonomy would be acquired in this regard through "secure technologies and solutions, alongside the ability to recognise and assess the opportunities and potential risks associated with digital technologies" (BMI, 2021, p. 22), which were translated within the action areas in different ways:

a) Applied research and development and the transfer of research (Action Area 1).
b) Cyber security “made in Germany” as a quality label (Action Area 2).
c) Government capabilities for assessing new technologies, commissioning European providers, and ensuring the self-protection of the public administration (Action Area 3).
d) A common EU vision and strategy for cyber security and European digital sovereignty (Action Area 4) (BMI, 2021, p. 22-23).

In this way, one can observe that Germany's digital mentality reinforced the country's scope of action within the European Union to avoid a more assertive position in its strategic surroundings.

Germany's preference to act within larger institutional frameworks, such as the EU, NATO, and OSCE, was also present in the new NCSS. Action area 4 indicated the country's will to have a more "active" role in shaping cybersecurity policy. Interestingly, no mention of the word "leader" on an individual basis was made. However, one can grasp a strong perception of norm shaping and the preference for a softer approach to achieve the idea of "power to control." In this regard, the link with conventional diplomatic power is evident.

Besides the normative element, capacity building was another feature raised. The NCSS mentioned Germany's will to strengthen confidence-building measures and capacity-building at bilateral and regional levels. In this regard, the strategy said the previous German efforts within OSCE on the agreed confidence-building measures. Moreover, on the issue of capacity building, it expressed the aim is to advance bilateral and regional cooperation on capacity building, […] so that the full potential of digital technology can be exploited and vulnerabilities can be reduced" (BMI, 2021, 115).

This outlook of the 2021 NCSS indicates that Germany's digital mentality involved more continuities than disruptions over the years. A self-perception based on sovereignty becomes apparent and can be interpreted as the maturation of the first ideas on the 2011 NCSS. Besides, the duality of security and economy was strengthened. At the same, even though not explicit, an element of norm entrepreneur[149] . This element of norm-entrepreneur can be inferred by the heavy focus on shaping norms and standards in the international sphere.

Still, one needs to recognize that recently the country has been more straightforward on measures against cyber attacks. Germany's position paper on how International Law applies to cyberspace exposed that "Germany agrees that cyber-related, as well as non-cyber related breaches of international obligations, may be responded to by both cyber and non-cyber countermeasures" (THE FEDERAL GOVERNMENT, 2021, p. 13). Besides, in 2022, the Federal Government stated that "As a "lead nation," Germany is leading a line of action to develop effective diplomatic instruments both to promote compliance and to build capacities." (DEUTSCHER BUNDESTAG, 2022b, p. 84, own translation)[150].

5.2 CYBER POWER PERCEPTIONS

Germany’s digital mentality has incorporated some elements of the German strategic culture, displaying more continuities rather than disruptions. Still, subtle shifts toward a more assertive approach to some topics could be traced over the years, starting from 2015. In this regard, a synthesis of Germany’s digital mentality can be seen in Table 11.

Despite the documents providing significant insights into Germany's digital mentality, the lack of direct mention of cyber power is striking. In this sense, a set of interviews was made to verify the assessment given by the document analysis. The interviews target BSI, BMI, BMVg, AA (*Auswärtiges Amt* – German Federal Foreign Office), and the Chancellery. Unfortunately, the potential interviewee from BSI did not receive clearance to interview. A similar case happened with the potential interviewee from BMI, who did not display time availability within the interview period despite having previous conversations to understand

[149] Generally speaking, the concept [of norm entrepreneur] refers to individual and collective actors who eagerly strive to promote the establishment, diffusion, and institutionalization of norms” (WUNDERLICH, 2020, p. 22).

[150] From the original in German: “Deutschland führt als „Lead Nation“ einen Handlungsstrang zur Entwicklung wirksamer diplomatischer Instrumente, um sowohl die Einhaltung von Normen zu fördern als auch Kapazitäten aufzubauen (DEUTSCHER BUNDESTAG, 2022b, p. 84).

the research in question (2020). Thus, successful interviews were conducted with an interviewee from AA (Interviewee D), BMVg (Interviewee E), and Chancellery (Interviewee F). From the three interviews, only the one with the AA was recorded. The other two were conducted orally, but the interviewees preferred to review their answers in a written manner.

Interviewee D highlighted a preference to use the term "influence" over "cyber power" in this regard. Indicating through the interview that having power would be related to "make other ones follow your will." Interviewee D stressed that the features of cyber power would include creating and maintaining a multistakeholder network, meaning a “network of international actors, which includes states, but also international organizations, companies, researchers, and academia.” Plus, some resources would include credibility, technical resource, personal resources, and size (ex., economic ties) (INTERVIEWEE D, 2020).

Interviewer D highlighted differences between the international and national fields of action during the interview. For Interviewee D, "Nationally, what cyber security agencies are dealing with is a technical matter. They are dealing with making society more resilient and fighting cybercrime. It is a completely different field of activity, exerting power or influence on an international level." (INTERVIEWEE D, 2020). In this regard, one can observe the rooted technical perspective on IT security within the German collective imaginary.

Besides, by considering the international field of action, Interviewee D explained that cyber power would differ from traditional national power. Interviewee D pointed to two elements of differentiation: "it is much less clearly defined what constitutes an attack on a country, militarily speaking." It "can be very difficult to identify the perpetrator behind a malicious cyber activity." In this regard, blurred lines and anonymity emerge as differentiation elements.

Thus, the different environment would imply a more restrained projection of power since, according to Interviewee D, "Projecting power may not be the most effective way of expressing power and influence because it can reduce your own credibility."In this sense, losing credibility and, thus, support within the needed networks would be a losing game. Besides, as Interviewee D stated, Germany would foster a democratic, not hierarchical, environment in cyberspace. According to Interviewee D (2020):

> We don't want to increase our power as a state actor, because we are a democracy. We don't want to accumulate power in our hands, so to speak, we want to restrict our own power. The same is true for the international field and Internet Governance.

Considering thus cyberspace as a democratic field, Interviewee D highlighted the importance of defense and deterrence. In this regard, Interviewee D (2020) explained that "in order to deter something, you don't need to have offense, but the capacity can react in different ways," which has been the base of German diplomatic reactions internationally.

Table 11 - Germany's Digital Mentality Summary

NCSS	Orientation	Threats Perceived	Self Perception	Investment (BSI)	Conventional Power Elements
2011	Techno-civilian approach	Criminals Terrorists States (espionage and military operations)	Technological sovereign country with an international coordination role in cybersecurity efforts and standards	€ 69 million	Military Economic Informational Diplomatic Political
2016	Global approach	Criminals Extremists/Terrorists States (military and intelligence)	Emerging cybersecurity technological and normative power	€ 88,7 million	Military Economic Informational Diplomatic Political
2021	Global approach	Cybercrime Cyber Terrorism Cyber espionage Cyber sabotage	Digital sovereign country and cybersecurity norm entrepreneur	€ 197 million	Military Economic Informational Diplomatic Political

Source: Own elaboration based on documents analyzed in the section.

Similarly, Interviewee F highlighted that Germany focuses on cyber resilience, preferring a motto based on "preventing in a non-aggressive way." Besides, departing from the perspective that the relationship between cyber power and states position would be paralleled, Interviewee F explained that Germany was transitioning, shifting its cyber mentality. It would be bringing together the two parallel systems "since it officially called for the use of the new EU sanctions regime to target Russian individuals (Dmitry Badin) following the 2015 hack attack against the German parliament's IT system" (INTERVIEWEE

F, 2020). This answer reinforces the idea of subtle digital mentality change grasped by the previous document analysis.

Besides, Interviewee F pointed out that cyber power elements would include financial resources, qualified staff, and strategy. In this regard, economy and human resources appear relevant. Interviewee F confirmed a view on "cyber operations as signaling and shaping a states' position cyberspace" when asked about the structure format of cyberspace in international relations. This view reinforces that projecting cyber power would not be the most desired outcome. Interview F stated that projecting and having cyber power would not necessarily be different, as, i.e., some provocations are "well done" and others "done for us to know.” This would not mean that there was no form of power projection.

Interviewee F acknowledges that "capacity development in other countries, by teaching, technical cooperation and development of systems would be ways of cyber power projection, once there would be transmission and shaping of ideas [behavior] to others [targets]." This element resonates with the German strategy toward cyber capacity building and a broader idea of cooperation as a fundamental pillar to maintaining a country's international status (INTERVIEWEE F, 2020).

Interviewee F also noted that “cyber power and national power can be detached, but especially with time, they won’t be much longer ("cyber is everywhere")” (INTERVIEWEE F, 2020). This idea was similarly presented by Interviewee E, in which cyber power and national power were interconnected. For Interviewee E, "power features could not be separated as many things suffered a digitalization process, for instance, Green Energy methods which are dependent on IT" (INTERVIEWEE E, 2020).

These blurred lines led Interviewee E also to treat the idea of cyber power as an influence. According to Interviewee E, "Germany's most effective way of protecting" things would be communicating (i.e., signaling capacity to the opponent). Besides, Interviewee E acknowledged a relationship between cyber power and states' position in the international system. However, he/she highlighted that it is "difficult to put a number on it"; it would depend on means of the influence of a country" (INTERVIEWEE E, 2020). In this regard, one can observe that Germany’s digital mentality having a softer approach can be confirmed.

Interviewee E highlighted that Germany had a "holistic" approach to cyber power. Besides, to maintain it, the country would base its action on three pillars: Defense (with BMVg), Internal Affairs (especially with BSI, dealing with critical infrastructures/building cyber resilience), and Diplomacy (having the AA in the center). Another interviewee confirmed Germany's preference for defensive rather than offensive action toward cyberspace in this sense.

In this regard, Interviewee E stated that, in his/her view, strong defensive capabilities were important to project cyber power (ex., security by design systems) and should weigh more than offensive capabilities. However, "this does not mean to discard offensive capabilities"(INTERVIEWEE E, 2020). This answer expresses Germany's attention to the military and its incorporation toward a more global approach.

Interestingly, despite coming from a military context, Interviewee E expressed that "it was good to highlight cyber diplomacy as a possibility for cyber power projection, at least for Western democracies. "He/she exposed that firstly diplomatic channels are attempted to solve conflict situations, and they are "quite effective nowadays" (INTERVIEWEE E, 2020).

In this regard, most of Interviewee E's answers matched the document analysis as some approaches Interviewees D and F provided. However, the most relevant point of Interviewee E was on the issue of cyber actors' capacity to achieve power in cyberspace. For Interviewee E, the evolution of computation (the Internet growth and spread, influence on standardization, etc.) gave the US a dominant role indicating a perceived asymmetry in achieving (cyber) power. Besides, for him/her, the strength of projecting power would also depend on a layered exploitation logic. The bottom layer would encompass the exploitation of known vulnerabilities; the second (intermediary) layer would encompass the exploitation of unknown vulnerabilities (e.g., Zero Days); the third layer would include the development/implementation of a weakness in the system (INTERVIEWEE E, 2020).

In this regard, Interviewee E explained that the third and upper layers would be the strongest position to project power, as it would provide a higher degree of certainty on effects caused by cyber operations (which the other layers could not offer). Besides, the strength feature of the third layer could be seen as only a "few nations have [this] capacity" (INTERVIEWEE E, 2020). This view shows a more technical and hierarchical perception of power, typical of the military lens.

On a final remark, the interviews highlighted that Germany was not considered a super cyber power. The perceptions displayed by all interviewees were that Germany was among great cyber leaders at an intermediary level since issues such as a heavily bureaucratic process make it difficult for Germany to have a proper pace with technological developments (INTERVIEWEE F). The heavy bureaucracy can also be an element in understanding the continuity of digital mentality in Germany, with the subtle shifts identified both in the documentation analyzed and the interviews.

5.3 PARTIAL CONCLUSIONS

The chapter showed that Germany varied its cybersecurity approaches in two main directions: techno-civilian and global. This variation showed a more constant change. Still, the country's threat and self-perceptions changed over time, demonstrating the evolution of the state's digital mentality. Germany's digital mentality is singular, grounded deeply in a restrained approach. In this regard, Germany's digital mentality led the country to assume an active position toward cyberspace with some glances of assertiveness. Besides, the chapter exposed that Germany pushes forward its cyber interests in a scattered way in policy forums, meaning that regionally it promotes the EU, assuming some traces in France related to strategic autonomy.

6 COMPARATIVE ANALYSIS OF CYBER POWER

Building upon the previous chapters, this chapter will have two primary goals. The first is to further develop comparisons between the case studies, highlighting common and different features between the UK, France, and Germany's digital mentalities. The second is to build upon these comparisons, shedding light on the concept of cyber power itself and paving the way (if possible) to broader inferences.

6.1 CYBER POWER FROM A CONSTRUCTIVIST PERSPECTIVE: STATE'S MEANINGS AND APPROACHES

To start a proper comparison between the UK, Germany, and France, one must first understand how these countries internationalize their digital mentalities. In other words, concepts of cyberspace, cybersecurity, and cyber defense can provide a big picture from the reasoning of these countries. The previous chapter drew some definitions from early NCSS and Defense documents. Here, we will recall them with a more in-depth analysis.

Starting with the concept of cyberspace, one can observe that the concept set in the first French NCSS remains almost unaltered over time. The definition of cyberspace as “The communication space created by the worldwide interconnection of automated digital data processing equipment” (ANSSI, 2011, p. 21) is the same as the ANSSI's digital glossary (ANSSI, 2022e). This loose concept allowed the country to incorporate defensive, security, and informational elements of cyberspace, which were concretely set in the LID, LIO, and L2I. On the other hand, the UK concept changed significantly over the years.

The 2009 NCSS explained that for the UK, cyberspace "encompasses all forms of networked, digital activities; this includes the content of, and actions conducted through digital networks" (CABINET OFFICE, 2009a, p.7). However, in the 2011 NCSS, the concept gained more tick descriptions. Cyberspace was considered "an interactive domain made of digital networks that is used to store, modify and communicate information," which would include "the internet but also the other information systems that support our [The UK] business, infrastructures and services" (CABINET OFFICE, 2011, p.11).

Still, in 2016, the concept was enlarged, including more hardware and immaterial elements. According to the 2016 NCSS, it was considered:

> the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, internet-connected devices and embedded processors and controllers. It may also refer to the virtual world or domain as an experienced phenomenon, or abstract concept (HMG, 2016, p.75).

Building upon this definition, a fourth one was set in the current NCSS. The definition was separated into a broader technical and military one, explaining that cyberspace could be understood by layers (virtual, logical, and physical) (HMG, 2021b, p. 19). According to the 2022 NCSS, in technical terms, cyberspace is "the interdependent network of information technology that includes the internet, telecommunications networks, computer systems, and internet-connected devices. "While for the military and considering the UK's efforts, it "is an operational domain, along with land, sea, air and space" (HMG, 2021b, p. 18). In this regard, the concept evolution within the UK shows a more open assertive position that the country took over the years.

For Germany, the concept of cyberspace has varied along a central idea. Still, the modification made in the 2016 NCSS is relevant because it tried to represent the same idea in a shorter version, as opposed to the UK. In this regard, the 2011 NCSS defined cyberspace as:

> the virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace (FEDERAL MINISTRY OF INTERIOR, 2011, p. 14).

The twist the 2016 NCSS gave in the original concept definition, which remained the same in the 2021 NCSS, was more toward the emphasis on data. Thus, for Germany:

> Cyberspace is the virtual area of all information technology systems in the world which are or could be interconnected at the data level. Cyberspace as a publicly accessible network is based on the internet, which can be expanded by means of any other data networks (BMI, 2021, p. 125).

One can observe by comparing these definitions that despite the different explanations of the concept, the countries analyzed have a common ground for understanding cyberspace. In this regard, all countries understand that cyberspace is broader than just the Internet or IT systems, encompassing software and hardware elements, and involving communications flows. From this base, the understanding of cybersecurity and cyber defense would be built on, already given some clues on developing the countries' digital mentalities.

In this regard, for setting early lines between defense and offense in cyberspace, France provided clear definitions for both concepts and intertwined them in its first NCSS. According to the Strategy, cybersecurity is:

> The desired state of an information system in which it can resist events from cyberspace likely to compromise the availability, integrity, or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible.
> Cybersecurity makes use of information systems security techniques and is based on fighting cybercrime and establishing cyberdefence (ANSSI, 2011, p. 21).

While cyber defense would be "The set of all technical and non-technical measures allowing a State to defend in cyberspace information systems that it considers to be critical (ANSSI, 2011, p. 21). The definitions set remained the same over the years, appearing as in the first NCSS in the digital ANSSI glossary (ANSSI, 2022e).

However, other concepts emerged along the strategic documents launched by France that complimented the country's understanding of defense and offensive elements. These would include the idea of active in-depth defense of cyberspace and a permanent cybersecurity posture. The first relates to "intrinsic systems projection with permanent surveillance, rapid response, and offensive action" (DÉFENSE ET SÉCURITÉ NATIONALE, 2008, p. 53, own translation)[151]. While the second would be related to the “strengthening of defence means and the development of offensive and defensive capabilities” (REPUBLIQUE FRANÇAISE, 2017, p.71).

Germany, by its turn, defined cybersecurity in its first NCSS through three lenses: global, civilian, and military. Interestingly, though, the concept of cyberdefense only appeared from the 2016 NCSS onward, being both the definitions of cybersecurity and cyber defense maintained from the 2016 NCSS to the 2021 NCSS. In this regard, the 2011 NCSS defines cybersecurity as the following:

> (Global) cyber security is the desired objective of the IT security situation, in which the risks of global cyberspace have been reduced to an acceptable minimum.
> Hence, cyber security in Germany is the desired objective of the IT security situation, in which the risks of the German cyberspace have been reduced to an acceptable minimum. Cyber security (in Germany) is the sum of suitable and appropriate measures.
> Civilian cyber security focuses on all IT systems for civilian use in German cyberspace. Military cyber security focuses on all IT systems for military use in German cyberspace (FEDERAL MINISTRY OF INTERIOR, 2011, p. 15).

[151] From the original in French: “combinant protection intrinsèque des systèmes, surveillance permanente, réaction rapide et action offensive” (DÉFENSE ET SÉCURITÉ NATIONALE, 2008, p. 53).

Interestingly this definition resembles some points of the French one, for instance, the statement that it would be the desired situation. Besides, by claiming German cyberspace, an idea of territoriality was also present.

The 2016 NCSS changed the definition of cybersecurity and introduced the idea of cyber defense, reinforcing the idea of a "whole of government" effort to secure cyberspace. In this regard, the 2016 and the 2021 NCSS explain that "cybersecurity is the IT security of all information technology systems which are and could be interconnected at data level in cyberspace" (BMI, 2021, p. 125). While cyberdefense would include

> […] the defensive and offensive capabilities in cyberspace that the Bundeswehr possesses to fulfill its constitutional tasks, and which are suitable and necessary for operational command or to avert (military) cyber attacks and thus to protect own information, IT, weapons, and other systems. This also includes the use and co-design of cyber threat prevention structures, processes and reporting in defence-relevant aspects and situations (BMI, 2021, p. 125).

The cyber defense definition shows a precise scope of action to create the divide between the Bundeswehr and BSI's roles. Moreover, it stresses ideas of proportionally and adequacy deployment of actions with the use of words "constitutional," "suitable," and "necessary," being part of the German strategic culture of self-restraint.

On the opposite side of restraint is the UK. The country's definition of cybersecurity present in the first NCSS was straightforward: "Cyber security embraces both the protection of UK interests in cyberspace and the pursuit of wider UK security policy through exploitation of the many opportunities that cyberspace offers" (CABINET OFFICE, 2009a, p. 9). In this regard, the definition by itself represents a means for a country to achieve its interests, an element that was reinforced in the text of the Strategy "It is important to remember that cyber security is not an end in itself" (CABINET OFFICE, 2009a, p. 9). Despite using both the terms cyberdefense and cybersecurity, the successor strategy has not described their definitions.

In this regard, only the 2016 NCSS would bring a new definition of cybersecurity. In this Strategy, cybersecurity referred to:

> […] the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures (HMG, 2016, p. 15).

Interestingly, a proper definition was still lacking despite using the term cyber defense. Still, the Strategy explained what Active Cyber Defence (ACD) meant. Therefore, ACD would be "the principle of implementing security measures to strengthen the security of a network or system to make it more robust against attack" (HMG, 2021, p. 74).

The latest, and current, NCSS practically maintained the definition of cybersecurity. It just added to the possibilities of unintentional harm manipulation. Thus, at the end of the description, the Strategy puts: "This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so" (HMG, 2021, p. 126). Meanwhile, ACD gained further explanation as a concept. According to the Strategy, ACD:

> […] helps organisations to find and fix vulnerabilities, manage incidents or automate disruption of cyber-attacks. Some services are designed primarily for the public sector, whereas others are made available more broadly to private sector or citizens, depending on their applicability and viability (HMG, 2021, p. 125).

This shift reflects the country’s situational awareness over the years, and its internal debate on the use of a whole-of-society approach (stated in the 2022 NCSS) since defense would include the participation of other actors besides the government.

This brief concept outlook shows that the countries' reasoning toward cyberspace, cybersecurity, and cyberdefense has evolved over the years. Notwithstanding some traditional elements in the countries, digital mentalities are noticeable. The first is the assessment of threats, classified among criminals, terrorists, and foreign/enemy states operations, especially regarding espionage.

In this regard, one must recall that all the strategies were launched after the 9/11 events in 2001. Despite the countries showing earlier concerns over IT security or data security in the digital domain, the impact factor of terrorism on the countries' threat perception is an element to take into account. Especially since the idea of cyberterrorism was already put in place in the late 1990s by Barry Collin, relating the possibility of terrorists' penetration of critical infrastructures systems to cause physical damage (COLLIN, 1997) and thus inflict terror among people. Moreover, state espionage and online criminal activity were already established in the 1980s.

One of the first known cyber incidents involving state-sponsored cyber espionage on US Department of Energy Laboratory systems was Cuckoo's Egg in 1987 (LIBICKI, 2021). Besides, cybercrime was already a reality in the 1980s with hackers' activities. One of the earliest and most known cyber criminals was Kevin Mitnick, who broke into the Digital Equipment Corporation Palo Alto Research Center and illegally duplicated the company's software, being charged and convicted for it in 1988 (MIDDLETON, 2017, p. 4). Therefore, these two types of threats were well known by states before they started to develop their digital mentalities properly.

In this regard, one must consider that the main weakness perceived by countries was thus related to critical infrastructures and sensitive data. The first one is set mainly because of the vulnerabilities embedded in industrial control systems (comprising SCADA[152], DCS[153], and PLCs[154]) that bring closer to reality cyber physical perils as a consequence, for example, cyber attacks that lead to network fragmentation or cascading failures (SHAKARIAN, SHAKARIAN; RUEF, 2013). Therefore, if it is the state’s traditional role to protect its citizens and the functioning of its society, and if critical infrastructures are essential to maintain society's functioning, thus, critical infrastructure protection or critical information infrastructure protection will be an obvious concern for states’. This is so, especially considering that most of the cyberspace infrastructure, which is often linked to these industrial control systems, is not owned by states but rather by private actors.

The second concern, protecting sensitive data, especially from espionage (whether from state or non-state actors’ espionage), also relates to maintaining states' social functioning and, more importantly, states' maintenance and strategic reasoning. In this regard, one must recall that when cyber espionage and cybercriminal activity emerged, the international context was the Cold War. Intelligence was, at that time, the key to proper situational awareness and strategic thinking. Besides, cryptography was a well-known method to protect states’ strategic communication being transferred to cyberspace since it was considered a new communication space (an aspect that the countries' definitions explained earlier made crystal clear). Thus, the concern on protecting systems using cryptography tools and the practice of breaking them to access classified information (as the Crypto AG case displayed in the previous chapter concretely showed).

The activities that states were already seen, attached to the weakness of IT systems in a Cold War context, shaped initial states' perception of the digital world. In this sense, Xuetong (2020) is correct when pointing out that a Cold War mentality is still influencing today’s decision-makers and that countries, considering the importance of the digital economy,

[152] Supervisory Control and Data Acquisition.
[153] Distributed Control Systems.
[154] Programmable Logic Controllers.

intertwined cybersecurity with it (what he claimed to be the two central elements of digital mentality)[155]. As the previous chapter showed, intelligence activity remains central to states, which can be considered a reminiscent aspect of the Cold War mentality, especially because of anonymity in cyberspace and, thus, the hardship of attribution. Indeed, the analysis showed that attribution is perceived more as a political decision than a technical one by all three analyzed countries. Public attribution seems like an efficient tool for the UK to shape behavior. While Germany and France do it under more discreet terms, France prefers bilateral dialogues, and Germany prefers to dissipate any sign of assertiveness within larger international policy forums, such as the European Union.

On the duality of security and the digital economy, the UK started its strategic reasoning with a market-driven approach, evolving to a more subtle link with technology innovation (industry and human resources development). While Germany and France initiated a more technical approach focused on industrial and human resources development. These elements can imply a perception of power going beyond a coercive/ approach (“power over”/ “power to control”) since innovation can be classified under the idea of protean power, relevant in uncertain contexts.

Moreover, the strategic documents sometimes stressed the countries as being digital nations. According to the UK's Office for National Statistics, in 2019, the country's size of the digital economy was £91.9 billion (ONS, 2022, p. 8), reaching 2020 the eighth position in the Digital Economy and Society Index (DESI) [156] (EUROPEAN COMMISSION, 2020c). Germany and France retrospectively ranked 12th and 15th in the 2020 DESI (EUROPEAN COMMISSION, 2020a; 2020b). The latest data version demonstrates an improvement in the ranking by Germany (jumping into the 11th position) while France maintained its rank in the 15th position (EUROPEAN COMMISSION, 2021a). The growing size of the digital economies in this sense matches the countries' efforts toward more investment into cybersecurity, discriminated in the previous chapter.

[155] For Xuetong (2020, p. 317), "Digital mentality refers to the way of perceiving and responding to international strategic issues from the perspective of cybersecurity and digital economy. It believes that, in the digital age, cyberspace is strategically more important to national survival than is the geophysical world—land, ocean, and air—and that digital superiority leads to global domination based on a nation's advanced digital economy and cybersecurity.

[156] This report includes country profiles, which help the Member States identify areas for priority action, and thematic chapters providing an EU-level analysis of the four principal policy areas, which group 33 indicators. The four priority areas analyzed are: Human Capital (Internet user skills and advanced digital skills), Connectivity (Fixed broadband take-up, fixed broadband coverage, mobile broadband, and broadband prices), Integration of Digital Technology (Business digitization and e-commerce), and Digital Public services (e-Government) (EUROPEAN COMMISSION, 2021b).

Regardless, to think about digital mentalities restricted to security and economic elements appears limited when one thinks of cultural components influencing states' perception of cyberspace. Cultural elements heavily influence states and date back to the Second World War, such as the restraining element in Germany's approach and France’s concept of strategic autonomy. The definitions of cybersecurity and cyber defense concepts are another layer of this argument since they appeared at different times for each country, indicating the nonexistence of a pre-established pattern but rather a constructed one.

The previous chapters demonstrated that all three countries encompass state power elements in their NCSSs. In this regard, beyond military and economic elements, diplomatic, informational, and political elements of conventional power come together into the equation. The fact that countries encompassed these elements can indicate how intertwined the digital world has become with the physical one and how this connection spills over to strategic state thinking.

Guarantee security in cyberspace cannot be considered isolated from national security. However, national security cannot be restricted narrowly to cybersecurity. In this regard, it is interesting that the three countries are set at different stages to prioritize cybersecurity in their national agendas. The political will comes along in this regard. It demonstrates that more than strategic goals and the known overall system weakness involving systems hacking (by non-state and state actors), the states' self-awareness played an important role, especially since an international multipolar order was established. The digital space opened new opportunities for states' to gain international relevance, at first, detached from geographical barriers. This self-awareness goes along with the idea set of self-perception as an element of the country's digital mentality. In this regard, a more encompassing concept of digital mentality allows one to embrace nuances that push forward or restrain the country's actions.

Therefore, thinking between external and domestic elements, typical of foreign policy, can demonstrate how threat perception (here called "the other") complements the self-perception idea. In this regard, despite the other being classified almost in a fixed manner between the UK, Germany, and France, the analysis showed a practice pattern related to significant cyber events that reverberated, if not in the strategic documents themselves, in the domestic debate over how to be positioned to combat threats. A summary of these patterns can be seen in Table 12.

The cyber events listed in Table 12 were referred to in the material analyzed in the previous chapter and do not encompass all the universe of cyber attacks that occurred worldwide. Notwithstanding, the case studies' mentioning indicates their relevance for the countries and their inception in the strategic thinking derived from threat perceptions. The cyber attacks against Estonia touched upon the imaginary toward cyberwar/cyber warfare. The Georgia conflict displayed the likelihood of combining conventional attacks with digital owns (in what countries, such as Germany, call hybrid threats). Stuxnet showed that even air gripped critical infrastructures systems could be hacked. The Snowden revelations triggered ideas of securing sovereignty (Germany and France), demanding greater transparency, and securing legitimacy (the UK). The TV5 and the Bundestag Hack demonstrated how critical targets related to communications (private and public) could cause social chaos. The US election interference shed light on protecting democratic processes from external actors, such as elections. Wannacry and NotPetya exposed the feasibility of collecting and reverting security tools to criminal activity (Eternal Blue). The COVID-19 pandemic opened the room to the increase of attack surface for malicious cyber actors, exposing issues such as social engineering, supply chain system dependencies, and data security.

It is important to highlight that this pattern formation does not relate solely to the weakness the threats displayed but rather to the set of self-perception, which can be translated to "what is my place/position in the world."This idea of placement is paramount to give a more assertive approach to countries, as a country would feel and want to demonstrate legitimacy in its action/posture. The assertive position relates to the public display of cyber offensive and attribution capabilities. In contrast, the active position refers to the development of capabilities to better prevent cyberattacks from occurring rather than just manage after-attack effects. The normative position, in its turn, goes to diplomatic efforts. In this regard, it is important to make clear that the table summarizes the most prominent features of countries' postures coming from the displayed weakness attached to the cyber incidents.

Table 12 - Countries' postures related to significant cyber incidents over the years 2007 -2022

Event/ Country	United Kingdom	France	Germany
Estonia cyber attacks	Reactive posture	Reactive posture	Reactive and normative posture
Georgia conflict	Active posture (focus on deterrence, + development of capabilities and intelligence)	Active posture (in-depth defense of cyberspace)	Reactive and normative posture
Stuxnet	Active and assertive posture (cyber attacks as priority risk + enhancement of cyber defense and deterrence capabilities)	Active posture (priority of cyber defense)	Active and normative posture (politicization of topic + multilateral focus)
Snowden Revelations	Active and assertive posture (transparency with security	Active posture (seeking greater autonomy in	Active and normative posture

	and intelligence Agencies)	cyber issues)	(seeking greater autonomy in cyber matters)
TV5 cyber attack/ Bundestag Hack	Active and more assertive (Active Cyber Defense and leadership role)	Active and assertive posture (development of offensive capabilities + greater platform regulation)	Active and normative posture with some assertive elements (whole of government task to secure and defend cyberspace)
US elections interference	Active and more assertive (Tackle fake news and protect elections)	Active and assertive posture (development of offensive capabilities + greater platform regulation)	Active and normative posture with some assertive elements (whole of government task to secure and defend cyberspace)
Wannacry/Not Petya	Active and more assertive (public attribution + sanctions+ further development offensive capabilities)	Active and more assertive posture (permanent cybersecurity and cyberdefense posture)	Active and normative posture with some assertive elements (further focus on research and intelligence)
COVID-19 (ransomware/supply chain attacks/ Doxing/ Cyber espionage)	Active and more assertive (cyber power concept + enhancement of attribution capability + cyber resilience)	Active and more assertive posture (cyber as a new domain for expression of power)	Active and normative posture with some assertive elements (sanctions + attribution+ active international role)

Source: Author's elaboration based on the analysis of Chapters 3, 4, and 5.

The table's patterns reveal a linear course of action the countries take toward more active and assertive postures. In this regard, it is worth noticing that all states started with a reactive posture. This does not mean that intelligence gathering was not a used tool. Rather it corroborates the countries' perception of cyberspace as more relevant while new communication and commercial venues. The three countries analyzed exposed at that time the lack of cohesion and thus unified strategic and operational thinking, which led to a more reactive position. Therefore, one can infer that at the beginning of the 2000's it seemed better for the countries to go along with the idea of passive defense in cyberspace while focusing on domestic developments (either creating new or enhancing old institutions).

The Georgia conflict marked the feasibility of military conflicts using cyberspace as a multiplier of force, which promptly triggered the UK and France to display their capacity to protect their societies effectively. On the other hand, Germany preferred to remain reactive, partly because it took longer to establish domestic cohesive defense actions properly and partly because it relied mainly on acting internationally within policy forums. In this regard, Germany only started to act actively after the Snowden revelations, mainly because of the domestic repercussion of an allied state (the US) hacking so closely on sensitive national information, especially the communications of a critical political actor such as Angela Merkel.

On the assertive position, in 2013, the UK was revealed to possess cyber strike capabilities through a statement by Philip Hammond, the defense secretary at the time. However, one must recall that already in 2012, on the occasion of the Olympic Games in London, the MoD set up a Joint Cyber Unit hosted by the GCHQ (CABINET OFFICE, 2012b, p. 3), and the 2011-2012 ISC report exposed that active cyber defense should be an opportunity to be exploited (ISC, 2012, p. 36). Further on, the 2016 NCSS effectively developed the idea of active cyber defense (HMG, 2016), nurturing the perception of cyber offensive and defensive capabilities as necessary and needing constant improvement. In this regard, the institutionalization of the National Cyber Force in 2020 (ISC, 2021) can be considered the highest point in an assertive position. In other words, it corroborates the almost linear progression of assertiveness from the country, which nonetheless included capabilities and tools such as public attribution and sanctions.

On France’s assertive position, one can recall the 2008 White Defense Paper installed the idea of national offensive capabilities development (DÉFENSE ET SÉCURITÉ NATIONALE, 2008) and that the 2013 White Defense Paper reinforced this idea (MINISÈRE DE LA DÈFENSE, 2013). Notwithstanding, the country only started to have a more assertive position in 2016, with the public declaration of Mr. Jean-Yves Drian of France's development of offensive capabilities and the establishment in 2017 of CYBERCOM (VIE PUBLIQUE, 2016). The country's assertiveness continues to grow, being further developed in the Defence and National Security Strategic Review (2018) and Cyber Defense and Offensive Policies (2019), mainly with the development of the "permanent cybersecurity posture" and the enhancement of the idea of cyber as a force multiplier (REPUBLIQUE FRANÇAISE, 2017; MINISTÈRE DES ARMÉES, 2019a; 2019b).

In its turn, Germany maintained a lower profile on its assertiveness. Despite implementing the Computer Network Operation unit, within the Strategic Reconnaissance Command, in 2007 (DEUTSCHER BUNDESTAG, 2015; STEIGER, 2022), only in 2012 was the country revealed to effectively have the capacity to conduct offensive cyber operations (DPA, 2012). Still, the country prioritized an international cooperation approach, changing its position to more "publicly assertive" with its "whole of government approach" set in the 2016 NCSS (BMI, 2016). These assertive elements grew with domestic development, such as

ZITIiS (2017) and Cyber-Agentur (2020), and were reinforced in the 2021 NCSS (BMI, 2021) and the latest statement made by the German Federal Government on Germany's attribution capability (DEUTSCHER BUNDESTAG, 2022b).

Comparing these developments, one can assume that 2015-2016 is a turning point for the country’s more assertive position (or at least as an important element). In this regard, one cannot infer that the cyber events displayed in Table 12 proportionate this position turn, but they can be identified as keystone marks to grasp states' strategic evolution. In other words, their digital mentalities evolved beyond the cyber events (that brought new perceptions of weakness into their realities) and new self-perceptions that directly influenced their international approaches to cyberspace and, more specifically, cybersecurity.

Besides, it is essential to highlight that despite the active and assertive positions relating to offensive and defensive capabilities development, other action venues were also developed. In this regard, the international engagement, and what Table 12 displays as a normative position for Germany, also gained greater weight in the states’ strategic thinking. All three countries understood the transnational cyberspace character, thus needing international engagement.

As stated in Table 12, Germany adopted a normative approach from the beginning of its involvement with cyberspace. Its first NCSS already mentioned the country's interest in being active in multilateral forums (FEDERAL MINISTRY OF INTERIOR, 2011), inserting its interests in states' behavior shaping. In this regard, the movement of drafting, with Brazil, a resolution within the UN on online surveillance that resulted in UNGA RES68/167 is a concrete example of this normative approach (JOYCE, 2015). Another great example was the country's role within OSCE in delivering agreed confidence-building measures (RMANIUCK; CLAUS, 2021). The international aspect permeated the two following NCSS (2016/2021) being framed within a regional scope (i.e., European). Moreover, its efforts to foster cyber dialogues with key partners are another venue to act discretely toward behavior shaping. Its position is to promote cyber capacity building and cyber confidence building measures worldwide (BMI, 2021).

The UK also acknowledges the international realm from the beginning of its strategic thinking. However, it considered cyberspace more as providing market opportunities, especially considering the 2009 and 2011 NCSS. The London Process (Global Conference on cyberspace) twisted this market approach slightly to the international realm when speaking of building "rules of the road. "Further on, the 2016 NCSS reinforced this idea, making it explicit that the UK would help in the building of state behavior (i.e., "rules of the road")

(HMG, 2016, p. 63). The public attribution practice is a concrete example of a more normative approach.

Notwithstanding, unlike Germany, the UK appears to mix the normative element within the broader scope of leadership roles and concepts of strategic advantage and power, as the 2019 GCHQ Director speeches demonstrated. As detailed in the previous chapter, the speeches highlighted defensive, offensive, and normative elements constituting cyber power. The Integrated Review (HMG, 2021a) and the 2022 NCSS (HMG, 2021b) also spoke of the international role of the UK, either as a valuable international partner to share values and uphold international norms (HMG, 2021a) or as a dimension of cyber power (HMG, 2021b).

France adopted, in a first moment, a more inward-looking when it came to cyberspace. The 2011 NCSS exposed that one of the action areas would include the development of international collaborations (ANSSI, 2011). However, only the 2013 White Paper would effectively mention the use of a diplomatic approach to attacks (MINISTÉRE DE LA DÈFENSE, 2013), white a proactive approach to include elements of surveillance as dual-use technologies on the Wassenaar Agreement, and a broader discussion among allies to establish a "code of conduct" related to data interception (DARWISH; ROMANIUK, 2021; SUEUR, 2014). The concerns over France’s autonomy and sovereignty gave a more focused agenda to France, encompassing its strategic surroundings (Europe and Atlantic allies). Notwithstanding, it calls attention that in 2017, the Defence and National Strategic Review exposed the question of attribution capability, which the previous chapter explained is not very open. Perhaps more relevant in the international realm was the launch of France's International Digital Strategy, mentioning in a similar way the UK's cyber power elements (mentioned by GCHQ's Director), pillars involving the economy, security, and governance. The follow-up activities of France would have a broader impact, such as the Paris Call in 2018 and the Strategic Review of Cyber Defense, which set among its principles to "act internationally in favor of a collective and controlled governance in cyberspace" (SGDSN, 2018a, p. 3).

In this regard, elements of security, economy, and international engagement (referred to as governance or diplomatic actions) build up the countries' perception toward cyberspace and, more interestingly, toward how to get an advantage and "get others to do what otherwise they would not. "Unsurprisingly, the first and second faces of power appear in the countries' positions. Nonetheless, it is interesting that self-perception also plays a fundamental role in position tendencies. The restrained culture of Germany, for instance, delayed a more active approach of the country despite the cyber events that impacted the other two countries, leading them to an active posture. Besides, the concern for autonomy triggered by the

Snowden revelations gave a deeper focus on domestic enhancements for France, that only started to broaden its actions with the perception of threats involving a more complex supply chain, which included foreign Platforms. The UK, by its turn, also had its global leadership past influencing an early active and assertive position.

On this issue, self-perception and threat perceptions appear valuable in understanding states' position in front of cyber events involving security. However, despite the different self-perception evolution, one can notice a pattern that emerged along the placement of assertive positions. This pattern is of global/holistic approaches to cybersecurity. Table 13 displays the countries' approaches evolution.

Table 13 - Countries’ approaches in comparison

Country/Year	2009	2011	2015/2016	2021/2022
United Kingdom	Market	Market	Government	Global
France	-------	Techno-military	Global	------
Germany	-------	Techno-civilian	Global	Global

Source: Author’s elaboration based on the analysis of Chapters 3, 4, and 5.

The global approach countries displayed in their NCSS is often referred to as the "whole of society" approach and indicates the perception of a relevant cohesive, coherent action path involving the different cyber actors. In other words, involving academia, the private sector, and government. In this sense, one can infer that all three states realize that cyber issues cannot be solely under the state's responsibility. This does not mean that the states were given up their control, but rather pushing forward a more inclusive agenda and opening the discussion table for other inputs. Still, this openness varies among the case studies. France, for instance, presents the paradox of being a “parent-state” when it comes to platforms regulations, while the UK reinforces the government as a central piece of organization and Germany, at the same time, opens up to other actors possess an intricate bureaucratic system that sometimes delays the pace of changes.

Another interesting point is that France and Germany took technical approaches in their first NCSS. Thus, in the first moment, pushing away further political engagements. The political will toward cyberspace and its defense and security in this regard were paramount. Until the three countries successfully politicized the subject, no significant enhancements, either domestically or internationally, were displayed.

Besides, the initial approaches of France and Germany, one more military directed and the other more civilian-oriented, clearly mark their strategic cultures, which, taken into a broader context, influence the European Union. This is so because according to the 2020 European Council of Foreign Relations (ECFR)'s Coalition Explorer survey,[157] 93% of the respondents considered France, while 97% considered Germany one of the most influential countries in EU policy (PUGLIERIN; FRANKE, 2020, p.10). As Puglierin and Franke (2020) point out, both countries could catalyze agreement between EU member states. This could include Digital Policy since it is a topic within both countries' top ten policy priorities, even if in different positions (for Germany, it is in the fourth position, while for France, it is in the ninth position).

The ability to gather states to agree on certain behaviors relates directly to the concept of power. In this sense, the key state actors' perceptions of cyber power gain further relevance. Not only in the European Union context but also within Europe as a region itself, which calls for attention to the UK, Germany, and France. Therefore, if digital mentalities, with the self-perception and the perception of the "other" (i.e., threats), can display states' position and approaches toward cyberspace and cybersecurity, it can also help one to understand how states' cybersecurity culture influences the construct of cyber power. The question of whether there can be common elements in this perception is further explored in the following subsection.

6.2 STATES' PERCEIVED ELEMENTS OF CYBER POWER

The only one who provided a detailed explanation of cyber power from the three case studies was the United Kingdom. The concept itself started to appear in the vocabulary of the UK in 2019, with two speeches by the GCHQ's Director, Jeremy Fleming. The ideas exposed by Fleming were that cyber power should be understood as a broader concept (beyond the Internet and technology) and related to a country's ability to influence others' behavior in cyberspace (FLEMING, 2019a, p. 4). In this regard, he pointed out that this influence could be achieved through defensive, offensive, and normative elements, stressing that a nation should be able to, if threatened, "project cyber power to disrupt, deny or degrade" adversaries

[157] "The Coalition Explorer is ECFR's flagship survey of European foreign policy experts and policymakers. It analyses the results of the biannual survey ECFR conducts in the EU27 (…) The 2020 edition is based on the expert opinions of 845 respondents" (PUGLIERIN; FRANKE, 2020, p. 3).

(FLEMING, 2019a, p. 4). Nevertheless, it should still consider issues such as necessity and proportionality.

Two years would have passed until the first official, open-sourced document explicitly used the term "cyber power," explaining what it meant to the UK. Therefore, in 2021, the Integrated Review of Security, Defence, Development and Foreign Policy described the concept, explaining that cyber power would be:

> […] the ability to protect and promote national interests in and through cyberspace: to realise the benefits that cyberspace offers to our citizens and economy, to work with partners towards a cyberspace that reflects our values, and to use cyber capabilities to influence events in the real world (HMG, 2021a, p. 40).

In this regard, the concept displayed the base elements of a digital mentality: security, economy, and international engagement. The document further develops the concept of explaining the effects of cyber power on the UK, which would be very similar to the ideas put on earlier by Mr. Fleming. Thus, the concept involved a defensive ("Cyber power protects our national security and resilience of our CNI [Critical National Infrastructure]) offensive ("It also creates new ways to pursue and protect our interests, enabling us to detect, deter, and disrupt our adversaries”) and normative approach (“[…] and to influence the global environment to ensure a safe and beneficial digital future for all”). Notwithstanding it also added an economic element to it, by saying it “supports economic growth, enabling business and individuals to transition confidently to the digital world, boosting productivity and driving the innovation that will create new skilled jobs”) (HMG, 2021a, p. 40).

In sequence, still in 2021, the launched 2022 NCSS would also highlight the idea of cyber power for the UK. The NCSS, in this sense, described cyber power as encompassing five broad dimensions related: to human resources (people, knowledge, skills, and partnerships), defense (the ability to protect assets through cyber security and resilience), economy (the technical and industrial capabilities), international engagement (the global influence, relationships and ethical standards to shape the rules and norms of cyberspace), and offense (the ability to take action in and through cyberspace to support national security, economic well-being and crime prevention) (HMG, 2021b).

Besides, the NCSS stressed two attributes linked to the UK as a cyber power: responsible and democratic, which would reinforce the country's vision of acting lawfully, based on international law, and proportionally. In this regard, it is interesting that the UK also stressed in the Strategy that cyber power projection would be "below the threshold of armed conflict and pre-conflict situations" (HMG, 2021b, p. 30). This position on power projection can be understood as the will to possess the capability of shaping other actions but not in such a way as to become a major threat to other states. Otherwise, the state in question would also become a major target for external attacks.

Compared to France and Germany, the UK bet boldly on displaying its will to become a cyber power since both countries had a more subtle approach to the topic. France used the term cyber power (*cyber puissance*) in more detail in the 2018 Strategic Review of Cyber Defense. According to the document, the state should have the ability and will to use capabilities beyond the possession of offensive and defensive capabilities. Besides, the description also points to an economic element: "Finally, it assumes that the State can rely on an industry able to relay and expand its action" (SGDSN, 2018b, p. 43). As described in the previous chapter, this economic element recalls the French strategic autonomy culture related to developing its own industrial capacity (DESFORGES, 2018) and the balance between independence and a strong Europe (LAUDRAIN, 2019a).

Germany, in its turn, has not described or used the term in any of the analyzed documents displayed in Chapter 5. However, this does not mean that the country does not possess an overall idea of the term and the concept itself. In this regard, and observing France's description, one can go back to the digital mentalities of the countries for a better understanding of key elements influencing the perception of "cyber power." Table 14 shows the tracked approaches.

One can observe that Germany's self-perception is grounded in two pillars: sovereignty and international engagement/norms promotion. These elements indicate a softer approach to the state's strategic culture of restraint. Moreover, they demonstrate what is relevant to the country regarding enhancing its security and displaying a solid position to other states. In this sense, if states prefer certain elements as more valuable than others, the ones the country chooses for itself will constitute features. It will look at others as a way of comparison and tracking relevance in the international realm.

Table 14 - Countries' cybersecurity approaches over the years in comparison

Country/Year	2009	2011	2015/2016	2021/2022
United Kingdom	Emerging Digital Economic Power	Consolidating Digital Economic Power	Cybersecurity leader and digital economic power	Leading Cyber Power
France	----	Emerging cyberdefense power	Digital Republic and cyber defense power	----

Germany	----	Technological sovereign country with an international coordination role in cybersecurity efforts and standards	Emerging cybersecurity technological and normative power	Digital sovereign country and cybersecurity norm entrepreneur

Source: Author’s elaboration based on the analysis of Chapters 3, 4, and 5.

This argument becomes more evident when one looks at the UK and France. Table 14 shows France has cyber defense power as an important self-assessment element. Within its explanation of what constitutes cyber power, it gave centrality to cyber defense capabilities, encompassing defense and offense. Besides, even if the industrial element was also mentioned in the French concept of cyber power, one can think of industry working toward developing cyber capabilities, as is the example of reliable cryptography.

The same goes for the UK definition of cyber power, which indicates a necessary leadership, focusing on the ability to set agendas internationally, and base further cyber developments on the economy (digital economy).

In this regard, states' self-perception becomes an interesting element in analyzing how cybersecurity cultures impact on country's definition of cyber power. When one understands the preferred elements, tendencies toward behavior can be potentially drawn. If one goes to the summary of data that the interviews provided, this idea becomes more evident. Table 15 exposes an overview of the interviewees' answers on the elements of cyber power and what it takes to protect and maintain it.

Table 15 - Interviewee's visions in comparison

Country	Interviewee	Cyber Power Elements	Cyber Power Projection	Maintenance of Cyber Power
United Kingdom	A (MFA)	*CNI Protection *Resilience *Intel. Capacity *Innovative private sector *Diplomatic infrastructures *Horizon Scanning	*Leading global position on laws and norms debate *Innovative cybersecurity private sector *Give the example of a resilient CNI *Scanning cybersecurity issues in emerging technologies	*Building coalitions *Have innovation credibility

France	B (MoD)	N/A	N/A	*IT industry to support cyber defense capability
	C (MFA)	*Capacities (offensive/defensive and of attribution) *Clear doctrine *Good administration *Innovation ecosystem	*Human resources *Cohesive international posture *Unifying approach	*Building coalitions *Multistakeholder approach
Germany	D (MFA)	*Creating and maintaining multistakeholder networks *Credibility *Technical Resources *Human Resources *Size (ex., economic ties)	*Cyber diplomacy (as a feasible way)	*Creating and maintaining multistakeholder networks *Credibility *Technical Resources *Human resources *Size (ex., economic ties)
	E (MoD)	*Main-fold spectrum (utilization of social networks/influence of public opinion, access to technical systems, manipulation of supply chains)	*Cyber diplomacy *Capabilities (defensive, signaling, and exploitation)	*Defense *Internal affairs *Diplomacy
	F (Chancellery)	*Financial resources *Qualified staff /Human resources *Strategy	Some Emerging Technologies (AI and 5G) Use of cyber proxies Cyber diplomacy Cyber Capacity Building	*Financial resources *Qualified staff /Human resources *Strategy

Source: Author's elaboration based on the analysis of Chapters 3, 4, and 5.

Table 15 demonstrates that all German interviewees considered cyber diplomacy an element of power projection. One can relate to the normative component of the state's vision *per se* of cyber power. Moreover, the elements to maintain and possess cyber power were set by two interviewees as the same. In this regard, it calls attention to the importance given to human and technical resources (which can be interpreted as cyber capabilities), and again "diplomacy" and the need for multistakeholder networks, created through credibility, as other relevant elements. The pillars explained by Interviewee E seem to summarize well the German understanding of cyber power. In other words, the concept would have the following elements: defense (here one can be considered both defense and offense capabilities); internal affairs (which can be translated into the idea of solid industry; sovereignty); and diplomacy (that encompasses credibility and the ability to create and maintain multistakeholder networks).

The elements exposed by the French interviewees indicate that good administration (which can be considered both at domestic and international levels) and cohesive international posture are necessary to possess and display cyber power. Besides, the views go along with the German idea of maintaining one's cyber power through networks/coalitions, which repeats itself in the English vision. Still, one can notice that the emphasis given to strengthening French's own industrial capabilities recalls its idea of strategic autonomy.

Interestingly, the idea of a solid autonomous industrial capacity reverberates to German reasoning, approaching both countries in the element of innovation. This could explain the pairing of both countries in projects that deal with emerging technologies development, such as Gaia-X. The French and German Economic Affairs presented this project in 2019. Within the European Union, it represents a significant effort toward building a (cloud) ecosystem “whereby data is shared and made available in a trustworthy environment” (GAIA-X, 2022). Another joint project that reflects the innovation element, and thus the strategic autonomy reasoning, is the joint calling for AI projects. The joint intent to develop a "Research and Innovation Network in Artificial Intelligence", was a development of the signature in 2019 of the Treaty of Aix-la-Chapelle, and the further intentions declaration signed between Ministry of Higher Education, Research and Innovation (*Ministère de l’Enseignement supérieur, de la Recherche et de l'Innovation,* MESRI) and the Federal Ministry of Education and Research (*Bundesministerium für Bildung und Forschung,* BMBF) (MESRI, 2020).

In this regard, one can infer that both the ideas of "power with" cyber capabilities and "protean power" are present in both countries. Still, from the interviewees, the reluctance to use the term "cyber power" became apparent. The emphasis on digital sovereignty can lead to this refrain since power and sovereignty historically were linked to unstable and warfare moments. The constructed perceptions, translated in narratives, over innovation, diplomacy, and sovereignty can thus explain that despite not mentioning (cyber) power *per se*, both Germans and French consider these elements to assess the degree of mightiness.

Interestingly the UK does not use the same terminology regarding sovereignty. Since 2018 the UK has pointed to having an issue with the use of the sovereign principle in the digital realm (SCHMITT, 2022). In its most recent statement on the application of international law, it explained that:

> The United Kingdom does not consider that the general concept of sovereignty by itself provides a sufficient or clear basis for extrapolating a specific rule or additional prohibition for cyber conduct going beyond that of non-intervention

> referred to above. At the same time, the United Kingdom notes that differing viewpoints on such issues should not prevent States from assessing whether particular situations amount to internationally wrongful acts and arriving at common conclusions on such matters. (THE UK, 2021, p. 4).

Therefore, as the UK does not use the term sovereignty for cyberspace, it allows it to use more freely the term cyber power. It essentially encompasses the same elements that Germany and France indicated. Still, to avoid the interpretation of "dominance," the UK uses positive reinforcement adjectives related to democracy and responsibility when using the word "cyber power."

The different views on power and its consequences become more evident when one observes the terminology preference between the analyzed countries. In this sense, to start thinking about protean power, embracing cyberspace as an uncertain environment can help better understand the concept of cyber power through the states' lens.

The different visions also impact states' self-international position assessment. While interviewees from France and the UK, when asked to rank their countries internationally and regionally, graded their countries with high scores (ranging between 8 and 9), German interviewees positioned the country in different ways, going from a high score to an intermediary one. Although not quantitative relevant, this result might indicate that the countries' self-assessment relying on the building of networks and proper cyber diplomacy[158] can lead them to better cooperate among themselves rather than assume a revisionist position. Thus, another element that can influence the choice of terms by France and Germany is that they do not recall power to avoid any misconception about dominance.

A final element worth mentioning is the states' treatment of the "other," meaning threats. Table 12 exposes the different positions the analyzed states assumed after disclosing new weaknesses. However, an element that showed itself persistent through the document analysis was the reference to risk mitigation. This approach to cyberspace acknowledges that total security is unachievable and reinforces the perception of cyberspace as an uncertain environment. It also enhances the idea of needed cooperation, especially through the construction of cyber capacity-building and confidence-building measures that both Germany and the UK explicitly displayed in their strategic documents.

Still, a question remains if one can observe states' positions and preferences regarding relevant elements of cyber power - to have it, project it or maintain it. Can one consider cyber

[158] According to Barrinha and Renard (2017, p. 355): “Cyber-diplomacy can be defined as diplomacy in the cyber domain or, in other words, the use of diplomatic resources and the performance of diplomatic functions to secure national interests with regard to the cyberspace”.

power as seen autonomously by states? Does cyber power stand on its own to shape others' will? The following sub-section will discuss this issue.

6.3 HAS CYBER POWER A CORE?

The idea of cyberspace as detached from other spheres of state control appears to be distant when one recalls the interviews, especially the ones with the Ministries of Foreign Affairs (MFAs) and all the strategic documents analyzed in previous chapters. The reasoning behind the action in cyberspace crosses diplomatic, informational, economic, and military spheres, and states acknowledge this. If one observes France's strategic documents, it explains several times that cyber has a multiplier effect (Cyber Defense Policy, International Digital Strategy, Cyber Offensive Military Doctrine). In its turn, Germany also considered in its White Papers (2006 and 2016) that the sole use of military actions would not be enough to provide cybersecurity. Along the same line, the UK exposed an encompassing line of thought, especially since it begone its digital mentality construction with a market-driven approach. Thus, one can assume that no coercive means by itself would be possible in cyberspace. In this regard, "power over" would not be feasible based solely on digital means.

Interestingly though, when one recalls the idea of protean power and the capacity of one to innovate, the scenario changes slightly. The idea of sovereignty attached to industrial production (i.e., autarchic emerging technologies development and deployment) can reflect on a sustainable and effective element capable of shaping other behaviors. Still, the digital economy cannot be confined to the cyber realm. The Internet of Things allows an increasing number of devices of the physical world to cross the digital and physical worlds. Besides, hardware components that allow the functioning of the digital space can also be incorporated into this reasoning, making, thus, impossible to separate cyber itself as economically relevant.

The informational and diplomatic spheres and the institutions existed before cyber, demanding physical interactions. The uniqueness of the open core of the Internet does not facilitate issues of power in cyberspace. Thus the complexity of the issue. After all, as the interviewees highlighted, networks and coalitions became relevant in an organized hierarchical international system. But, states in this regard try to avoid bringing too much hierarchization into cyberspace to maintain stability.

Therefore, conventional and digital elements mesh together, maintaining two parallel worlds functioning, the physical and the digital. These worlds complement each other, and for both to survive, taking into account the degree of digitization of many societies, both need to feed them back. In this sense, to think of conventional powers as more relevant to assess a state cyber power becomes unreasonable, as the important elements emerge from the intertwining between the two worlds.

6.4 PARTIAL CONCLUSIONS

The chapter showed that one could assume that an idea of digital mentality that does not encompass the self-perception of countries becomes limited. Analyzing self-perception can help one understand some states' position in front of vulnerabilities. It can also shed light on the topic, bringing similar concepts related to power ideas and why some states use the term cyber power (the UK) while others do not (Germany and France). Moreover, a constructivist approach contextualized and displayed states' strategic thinking toward cyberspace. Thus helping one to understand that strategic culture, dating before the Cold War, influences states. This influence goes into states' perceptions of cyberspace and shapes what countries value as synonyms of might in the digital sphere.

The chapter highlighted that the shared pillars of cyber power are: security/defense, governance, and economy. In this regard, it becomes clear that cyber power is seen more as "influence" than "coercion," despite being intertwined in all conventional powers spheres. In other words, cyber power cannot be assumed to be an autonomous element for states as its immaterial elements are attached to physical ones to impact the physical world.

7 CONCLUSION

Cyber power is a complex concept that deserves more attention from scholars and policymakers. Power by itself can assume multiple forms and be conceptualized differently depending on the ontological grounds that base this concept. In this regard, the Introduction (Chapter 1) highlighted that the uniqueness of cyberspace poses challenges to states, especially in understanding how power relations manifest themselves in this digital environment.

Security and stability in cyberspace are well-grounded goals that require states to act strategically based on perceptions. These perceptions usually are disregarded when one thinks about structured studies on power in cyberspace. Therefore, the thesis seeks to shed light on this gap, questioning: How do states' perceptions of cybersecurity shape the form of their power projection? Does that confer a new form of power relations, therefore, cyber power as a phenomenon? Based on these questions, the research aimed to identify what elements states perceive to be the base of cyber power and how this perception influences states' preference for cyber power projection.

The research was framed as a qualitative comparative study with a case-centered design being the cases selected in the United Kingdom, France, and Germany to reach proper conclusions. Chapter 1 then further explained the methodology and division of the study's chapters. In this regard, Chapter 2 recalled, through literature review, how relevant Political Science is for International Relations ontologies and how these ontologies shaped power concepts that spilled over into cyberspace, culminating in a few cyber power theories.

The idea of cyber power has evolved in the last few decades in what can be classified into two theory generations: one more realist and the other more liberal (CAVELTY, 2018). Still, what appears to be the third generation is emerging, showing a more constructivist approach. This constructivist generation of cyber power theories focuses on incorporating qualitative studies insights, proposing a different look toward the phenomenon of cyber power. Building on this approach, Chapter 2 further explains the thesis' research design would use an eclectic formulation to analyze the case studies. Therefore, ideas of "power to control" and "protean power" displayed by Katzenstein and Sybert (2018), and ideas from the International System functioning derived by Alexander Wendt (1999,1992), in which is understood that cyberspace is what states make of it, would be put in place to grasp states perception toward cyberspace. In this regard, the research departed from the element of agency, not the structure itself, focusing on how state perceptions shape digital reality.

The idea of digital mentality was presented in Chapters 3, 4, and 5, encompassing states' self-perception and the perception of the other (i.e., threats). In this regard, the Chapters detailed the evolution through time of the United Kingdom, France, and Germany's digital mentalities. They looked beyond the countries' national cybersecurity strategies to grasp perceptions and thoughts over cyberspace, cybersecurity, and cyber power.

Chapters 3, 4, and 5 also framed insights into orientation, perceived threats, self-perception, investment, and conventional power. The orientation category discriminated against countries' main approaches and National Cybersecurity Strategies. The threats perception category encompassed repeated threat instances found in documents. The self-perception category described the overall points that the document analysis pointed to regarding the state's self-denomination, role, or aimed projection. The investment category sought to gather the amount designated to cybersecurity/cyber defense in the documents. The conventional powers category related to the areas that the NCSS encompassed, resembling conventional states' powers (Diplomatic/Political, Informational, Economic and Military, or DIME).

Moreover, the individual case study chapters showed some key cyber events that changed states' approaches and their repercussions on international and domestic levels. This point reinforces the idea of the co-creation of agency and structure recognized in constructivist approaches. Additionally, the interviews gathered with representatives of crucial cybersecurity agencies of each country demonstrated that the empirical data gathered matched the document analysis. In this sense, and despite the limited number of interviews, some key confirmations and aspects that were not addressed in the strategic documents analyzed were possible. One good example was the interviewees' answers on the configuration of the international digital system, which did not resemble the physical one. Other elements of interest for the research involved ideas of gaining, maintaining, and projecting cyber power.

Chapter 6 wrapped the information displayed in Chapters 3, 4, and 5, developing a series of comparisons. The comparisons showed the cases' linear course of action toward more active and assertive postures (i.e., attribution and offensive capabilities public display) related to cybersecurity. All states started with a reactive posture to cyber events, corroborating the countries' initial perception of cyberspace as more relevant, while new communication and commercial venues. This initial posture can also be considered a result of the country's initial lack of cohesion and, thus, unified strategic and operational thinking.

Besides, even though cyber power was a term only used explicitly by the UK, its idea was translated into the term sovereignty (used by France and Germany).

In this sense, the duality of security and economy was well presented, but an essential element of "influence" was raised. The interviewees demonstrated this influence aspect more straightforwardly, which exposed that cyber power projection would be visible through diplomacy/cyber diplomacy. By recalling the second power face, one can infer that soft skills and institutional frameworks gain relevance, especially if one considers the lack of human resources pointed out through some documents and interviewees. Therefore, countries lagging in cyber diplomacy issues would implicate lower power status regarding those with the staff and soft capabilities developed for such endeavors. This a problem, especially in Latin America, that should be considered, and even more in countries such as Brazil that are in the early stages of formalizing cyber diplomacy as a Ministry of Foreign Affairs permanent track.

Chapter 6 also pointed out that the three studied states acknowledged cyberspace's configuration as a conflict domain but bet on norms and international law to avoid instability. This behavior confirms the challenges for states (at least Western ones) in applying democratic principles to the international digital system to prevent an excessive hierarchy. Therefore, constructivist approaches can better depict the constructed reality regarding power rankings. The best way forward is to group states into broader categories, such as Tiers, as the International Institute for Strategic Studies Net Assessment.

Chapters 3, 4, 5, and 6 demonstrated that strategic culture contributes to states' perceptions and cybersecurity. In this sense, ideas of the Cold War can be noticed in the relevance of intelligence given by all three states, but also ideas developed after the Second World War were still much present. These ideas can be seen in larger regional contexts, such as the European Union and the North Atlantic Treaty, the preferred policy forums of the three states analyzed. In this regard, further regional research on cyber power would be interesting to be pursued. Significantly deepen the relationship between individual interests and bloc position in international physical and digital systems.

Strategic cultures dating from a previous international context can partly explain state focus on emerging technologies. Innovation through the industry (hardware and software) comes along with acknowledging cyberspace as an uncertain environment. The stealthiness that cyberspace creates, making it challenging to assess concrete capabilities (such as the number of cyber weapons a country posses), was converted into attention to issues, such as attribution capacity and horizon scanning. An aspect that links with techno policy and geopolitics ideas involving the development of Artificial Intelligence, Quantum Computing, Cloud Computing, and so on.

The merge of technology and cyberspace reinforces the idea of parallel worlds complementing each other, cemented by the digital economy and the increasing society's dependency on the digital realm. In this regard, the research showed that cyber power is not a changing driver of international polarity but can indeed help in polarization – especially if one recalls ideas of splinternet.

Splinternet is the idea of the Internet splitting up "into a collection of fragmented networks controlled by governments or corporations." (YORK, 2022). Still, as Mueller (2017, p.33-34) explains, the real debate behind it is "a power struggle about which units of the Internet are truly autonomous (self-governing) and which ones are subordinate." In this regard, Mueller (2017) exposes that the debate is between those who advocate for greater state control over the Internet (alignment) and those who support technical efficiency and user demand-driven Internet (self-determination), falling directly into ideas of sovereignty over cyberspace.

Therefore, considering international actors' tendency to cluster around the most powerful states (polarization) and the perception of states as cyber powers, one can recall the answer of Interviewee A on polarized cyberspace on West and East visions. Thus, one can infer that cyber power can push forward polarization structures. This could be a reasonable reason for Germany's and France's cautiousness with the concept of cyber power itself.

However, concretely, cyber power, while an identity aspect, is still in formation. It appears to relate directly to International Law, norms, and ideas such as sovereignty. But then, again, how sovereignty shall properly apply to cyberspace remains a mystery. The cases studied in this thesis displayed that states do not agree on the matter since the UK does not consider the application of the sovereignty principle over cyberspace, while Germany and France do. Therefore, further research on it would also be interesting to be explored.

Considering this aspect, how strategic security cultures in different regions, such as Asia, Latin America, the Caribbean, and Africa, influence perceptions over sovereignty, diplomacy, and power relations in cyberspace are open lines of research worth developing. This is especially so as states in different regions demonstrate different behaviors in cyberspace. In Latin America and the Caribbean, for instance, states are framed as "swing states" (MORGUS *et al.*, 2019), as they align more pragmatically either with West or East states on international policy forums regarding a variety of cyber issues.

In this regard, the present thesis was just a first frame of the debate, departing from a small sample of European countries' analysis, which thus imposes a limit on generalizations. Still, the in-depth qualitative analysis of a small sample of countries opened up a poorly explored vision of cyber power and power relations in cyberspace: a constructivist one. The constructivist approach can shed light on the open questions raised and lead to more robust, empirically grounded research on cyberspace and its dynamics.

In sum, this thesis exposed that digital mentalities affect states' perception of their cyber power projection. In other words, states' perception of cybersecurity shapes the way they view their form of power projection as it brings an understanding of the blending of the physical and digital world. This blending brings up a space of risks and uncertainties, leading to ideas of "power to control" and "protean power." Besides, this space creates a new reality for states' self-perceptions, a (not so) hierarchical structure influenced by different conventional strategic cultures, giving a softer approach to cyber power projection to the studied cases. Thus, the cases used in the research (which can be broader to Western countries) fixed on cyber diplomacy and influence as critical core concepts to power projection. This is not a revolutionary thought, as movements on international policy forums such as the UNGGE and OEWG have been in motion for some time now. Therefore one can affirm that cyber power as a phenomenon is still maturing. Still, better understanding the link between diplomacy and power, taking into account not only innovation but also control, can be an excellent path to understanding the phenomenon of cyber power and thus place states accordingly in an international framework.

REFERENCES

ADAM, Patricia.; BAS, Philippe. **Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016.** Assemblée nationale: Sénat, 2017. Available at: http://www.senat.fr/rap/r16-448/r16-4481.pdf . Last access: May 22, 2022.

AGENCE DE LA SÉCURITÈ DES SYSTÈMES D'INFORMATION - ANSSI. **VIGIPIRATE**. 2022a. Available at: https://www.ssi.gouv.fr/alertes/vigipirate/. Last access: May 9, 2022.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION - ANSSI and BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK - BSI. **Third edition of the Franco-German common situational picture**. Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2020. Available at: https://www.ssi.gouv.fr/uploads/2020/12/anssi-bsi-common_situational_picture_2020.pdf Last access: May 23, 2022.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION - ANSSI and BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK - BSI. **Second edition of the Franco-German common situational picture**. 21st May 2019. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/D-F_Reports/Common_Situational_Picture_2019.pdf?__blob=publicationFile&v=1.Last access: May 23, 2022.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION - ANSSI. **Une Année 2021 Marqué par la Professionalisation des Acteurs Malveillants.** 03 March 2022b. Available at: https://www.ssi.gouv.fr/actualite/une-annee-2021-marquee-par-la-professionnalisation-des-acteurs-malveillants/ . Last access: May 23, 2022.

AGENCE NATIONALE DE LA SÈCURITÉ DES SYSTÈMES D'INFORMATION - ANSSI. **Glossaire.** 2022e. Available at: https://www.ssi.gouv.fr/entreprise/glossaire/ .Last access: July 11, 2022.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION - ANSSI. **Information systems defence and security France's strategy.** Paris, 2011.Available at: https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf. Last access: May 22, 2022.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION - ANSSI. **Manifeste pour l'ANSSI des 10 prochaines années; pour l'écosystème de la cybersécurité**. 21 January 2020b. Available at: https://www.ssi.gouv.fr/uploads/2020/01/anssi-manifeste-2020.pdf . Last access: May 9, 2022.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION - ANSSI. **Papiers numériques**. Paris: Agence Nationale de la Sécurité des Systèmes d'Information. 2020a. Available at: https://www.ssi.gouv.fr/uploads/2020/06/anssi-papiers_numeriques-2020.pdf . Last access: May 22, 2022.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D’INFORMATION - ANSSI. **Rapport d’activité 2015**. Paris: ANSSI, 2016. Available at: https://www.ssi.gouv.fr/uploads/2016/09/rapport_annuel_2015_anssi.pdf . Last access : May 22, 2022.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D’INFORMATION - ANSSI.**France Relance Volet cybersécurité FAQ ANSSI**. 2022d. Available at: https://www.ssi.gouv.fr/agence/cybersecurite/france-relance/le-volet-cybersecurite-de-france-relance-faq/ . Last access: May 23, 2022.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D’INFORMATION - ANSSI.**Panorama de la Menace Informatique 2021**. 9 March 2022. Available at: https://www.cert.ssi.gouv.fr/uploads/20220309_NP_WHITE_ANSSI_panorama-menace-ANSSI.pdf. Last access: May 23, 2022.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D’INFORMATION - ANSSI. **Rapport d’Activité 2016**. Paris: ANSSI, 2017. Available at: https://www.vie-publique.fr/sites/default/files/rapport/pdf/184000261.pdf. Last access : May 23, 2022.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D’INFORMATION -ANSSI. **Rapport d’Activité 2017.** Paris: ANSSI, 2018. Available at: http://www.sgdsn.gouv.fr/rapport_annuel/rapport-dactivite-2017-anssi/ . Last access: May 9, 2022.

ANDERSON, Steven J. **Air power lessons for an Air Force Cyber Power Targeting Theory**. Drew Paper No. 23. Maxwell Air Force Base, Alabama: Air University Press, Air Force Research Institute, 2016.

AREVA. **AREVA S.A. Accompanies AREVA’S Corporate Restructuring.** 2022. Available at: https://www.sa.areva.com/EN/home-57/areva-s-a.html. Last access: 22 May 2022.

ARMS CONTROL ASSOCIATION. **The Wassenaar Arrangement at a Glance**: Fact sheets and Briefs. February 2022. Available at: https://www.armscontrol.org/factsheets/wassenaar. Last access: May 22, 2022.

BACHRACH, Peter.; BARATZ, Morton S. **Power and Poverty:** theory and practice. New York: Oxford University Press, 1970.

BACHRACH, Peter.; BARATZ, Morton S. Two Faces of Power. **The American Political Science Review,** v. 56, n. 4. Dec. 1962, pp. 947-952

BAEZNER, Marie. France. *In:* DEWAR, Robert S (ed). **National Cybersecurity and Cyberdefense Policy Snapshots:** Collection 1. Zürich: Center for Security Studies (CSS), ETH Zürich, September 2018.

BALDWIN, David A. Power and International Relations. *In:* CARLSNAES, Walter.; RISSE, Thomas.; SIMMONS, Beth A. Simmons. **Handbook of International Relations.** 2nd Ed. Thousand Oaks, CA: SAGE Publications, 2013. p. 273-297.

BARCOMB, Kris E. From Sea Power to Cyber Power: learning from the past to craft a strategy for the future. **Joint Force Quarterly**, v. 69, 2nd quarter 2013.

BARNETT, Michael. DUVALL, Raymond. Power in International Politics, **International Organization,** v. 59, n.1, 2005. p. 39-75.

BARRINHA, André.; RENARD, Thomas. Cyber-diplomacy: the making of an international society in the digital age. **Global Affairs**, v. 3, n. 4-5, 2017. pp. 353-364. DOI: 10.1080/23340460.2017.1414924

BAS, Philippe. **Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2017.** Assemblée nationale: Sénat, 2018. Available at: https://www.senat.fr/rap/r17-424/r17-4241.pdf. Last access: March 27, 2022.

BBC News. **UK launched cyber-attack on Islamic State.** 12 April 2018. Available at: https://www.bbc.com/news/technology-43738953. Last access: March 27, 2022.

BEBBER, Robert. Cyber Power and Cyber Effectiveness: An Analytic Framework. **Comparative Strategy,** v. 36, n. 5, 2017. pp. 426-436.

BEIGEL, Rebecca.; HERPIG, Seven. **Germany's Cybersecurity Architecture** [Translation of the 6th German edition]. Berlin: Stiftung Neue Verantwortung. April 2021. Available at: https://www.stiftung-nv.de/sites/default/files/eng_impulse-germanys_cybersecurity_architecture_translation_of_the_6th_german_edition_0.pdf. Last access: June 20, 2022.

BENDIEK, Annegret.; SCHULZE, Matthias. Attribution: A Major Challenge for EU Cyber Sanctions. An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW **SWP Research Paper** 2021/RP 11. Available at:https://www.swp-berlin.org/en/publication/attribution-a-major-challenge-for-eu-cyber-sanctions. Last access: June 21, 2022.

BERGER, Thomas. U. **Cultures of Antimilitarism. National Security in Germany and Japan**, Baltimore, MD: Johns Hopkins University Press, 1998.

BETZ, David J.; STEVENS, Tim. **Cyberspace and the State:** towards a strategy for cyber-power. London: The International Institute for Strategic Studies (IISS), 2011.

BLITZ, James. UK becomes first state to admit to offensive cyber attack capability. **Financial Times (online)**, 2013. Available at: https://www.ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de. Last access: March 27, 2022.

BOCKEL, Jean-Marie. **Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur la cyberdéfense**.Strasbourg, France Available at: https://www.senat.fr/rap/r11-681/r11-6811.pdf .Last access: May 22, 2022.

BÖHLE, K. **Enquete-Kommission "Zukunft der Medien in Wirtschaft und Gesellschaft-Deutschlands Weg in die Informationsgesellschaft" auf den Weg gebracht**. TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis, DE, v. 5, n. 1, p. 25–26, 1996.

DOI: 10.14512/tatup.5.1.25. Available at: https://www.tatup.de/index.php/tatup/article/view/4656 .Last access: May 24, 2022.

BONNER, E. Lincon. **Cyber Power:** attack & defense lessons from land, sea, and air power. 2011. Graduation Thesis - Faculty of the School of Advanced Air and Space Studies, School of Advanced Air and Space Studies Air University, Maxwell Air Force Base, Alabama. Available at:https://webcache.googleusercontent.com/search?q=cache:_fVEkvFmZzEJ:https://www.hsdl.org/%3Fview%26did%3D812459&cd=1&hl=pt-BR&ct=clnk&gl=br. Last access: May 24, 2022.

BOTEK Adam. **European Union establishes a sanction regime for cyber-attacks**. 2019. Available at: https://ccdcoe.org/library/publications/european-union-establishes-a-sanction-regime-for-cyber-attacks/. Last access: March 27, 2022.

BOZZ ALLEN HAMILTON INC. **Cyber Power Index**. 2011. Available at: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/eiu-cyber-power-index-findings-and-methodology. Last access: March 26, 2019.

BULL, Hedley. **The Anarchical Society:** a study of order in world politics. London and Basingstoke: Macmillan, 1977.

BUNDESAMT FÜR SICHERHEIT IN DER INFORAMTIONSTECHNICK - BSI. **CERT-Bund**. 2022b. Available at: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html. Last access: June 20, 2022.

BUNDESAMT FÜR SICHERHEIT IN DER INFORAMTIONSTECHNICK - BSI. **Historie des BSI.** 2022a. Available at: https://www.bsi.bund.de/DE/Das-BSI/BSI-Historie/bsi-historie_node.html; Last access: June 20, 2022.

BUNDESAMT FÜR SICHERHEIT IN DER INFORAMTIONSTECHNICK - BSI. **Kurzprofil des BSI**. 2022c. Available at: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/BSI-Kurzprofil/kurzprofil_node.html. Last access: June 21, 2022.

BUNDESGESETZBLATT TEIL I NT. 25. **Zweites Gesetz zur Ërhohung der Sicherheit informationstechnischer Systeme.** 27 May 2021. Available at: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1654980725451 . Last access: June 21, 2022.

BUNDESMINISTER DER FINANZEN - BMF. **Haushaltsrechnung des Bundes für das Haushaltsjahr 2011.** 2011. Available at: https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Oeffentliche_Finanzen/Bundeshaushalt/Haushalts_und_Vermoegensrechnungen_des_Bundes/haushaltsrechnung-und-vermoegensrechnung-des-bundes-Haushaltsrechnung-2011.pdf?__blob=publicationFile&v=4. Last access: June 21, 2022.

BUNDESMINISTER DER FINANZEN - BMF. **Haushaltsrechnung des Bundes für das Haushaltsjahr 2016 (Band 2)** 2016. Available at:

https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Oeffentliche_Finanzen/Bundeshaushalt/Haushalts_und_Vermoegensrechnungen_des_Bundes/haushaltsrechnung-2016-band-2.pdf?__blob=publicationFile&v=5 . Last access: June 21, 2022.

BUNDESMINISTERIUM DER VERTEIDIGUNG - BMVg. **Verteidigungspolitische Richtlinien Nationale Interessen wahren** –Internationale Verantwortung übernehmen – Sicherheit gemeinsam gestalten. 2011 - Verteidigungspolitische Richtlinien. Bonn: BMVg, July 2011. Available at: https://www.bmvg.de/resource/blob/13568/28163bcaed9f30b27f7e3756d812c280/g-03-download-die-verteidigungspolitische-richtlinien-2011-data.pdf . Last access: June 21, 2022.

BUNDESMINISTERIUM DER VERTEIDIGUNG - BMVg. **Weißbuch 2006 zur Sicherheitspolitik Deutschlands und zur Zukunft der Bundeswehr**. Berlin: Bundesministerium der Verteidigung, October 2006. Available at: http://archives.livreblancdefenseetsecurite.gouv.fr/2008/IMG/pdf/weissbuch_2006.pdf. Last access: June 20, 2022.

BUNDESMINISTERIUM DES INNEN, FÜR BAU UND HEIMAT - BMI. **Nationaler Pakt Cyber Sicherheit. Online Kompendium Cybersicherheit in Deutschland**. Berlin: Bundesministerium des Innern, für Bau und Heimat, November 2020. Available at: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/it-digitalpolitik/online-kompendium-nationaler-pakt-cybersicherheit.pdf;jsessionid=B21A701CE664B80A82252595C1B551A7.2_cid364?__blob=publicationFile&v=8. Last access: June 21, 2022.

BUNDESMINISTERIUM DES INNER - BMI. **National Strategy for Critical Infrastructure Protection (CIP Strategy)**. Berlin, 17th June 2009. Available at: https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf;jsessionid=303DEE5261E10C36729C27A3BEEDB4AC.1_cid364?__blob=publicationFile&v=1. Last access: June 21, 2022.

BUNDESMINISTERIUM DES INNER - BMI. **Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI).** Berlin: Pinguin Druck,. July 2005. Available at: https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/05-12-09/05-12-09-anlage-nr-16.pdf?__blob=publicationFile&v=2 . Last access: June 21, 2022.

BUNDESMINISTERIUM DES INNER - BMI. **Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen**. 2007. Available at: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/umsetzungsplan-kritis.pdf;jsessionid=18F68DCEF5F71BA4B92C58256CC9394C.1_cid364?__blob=publicationFile&v=4 . Last access: June 21, 2022.

BUNDESMINISTERIUM DES INNER - BMI. **Cyber-Sicherheitsstrategie für Deutschland 2016**. Berlin: BMI, November 2016. Available at: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf . Last access: June 21, 2022.

BUNDESVERFASSUNGSGERICHT - BVerf. **Judgment of the First Senate of 27 February 2008** - 1 BvR 370/07 -, paras. 1-333. 2008. Available at: http://www.bverfg.de/e/rs20080227_1bvr037007en.html. Last access: June 21, 2022.

BUNDESWEHR. **Kommando Strategische Aufklärung.** 2022. Available at: https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-strategische-aufklaerung. Last access: June 21, 2022.

BUSINESS FRANCE. **Presentation of the "France 2030" plan 2021**. 15 October 2021. Available at: https://www.businessfrance.fr/discover-france-news-presentation-of-the-france-2030-plan. Last access: May 22, 2022.

BUZAN, Barry.; LITTLE, Richard. **International Systems in World History**: remaking the study of international relations. New York: Oxford University Press, 2000.

CABINET OFFICE. CENTRAL SPONSOR FOR INFORMATION ASSURANCE. **A National Information Assurance Strategy**. 2007. Available at: https://silo.tips/download/central-sponsor-for-information-assurance-a-national-information-assurance-strat. Last access: March 27, 2022.

CABINET OFFICE; MAUDE, Francis. **UK Cyber Security Strategy:** statement on progress 2 years on (Written statement to Parliament). 2013. Available at: https://www.gov.uk/government/speeches/uk-cyber-security-strategy-statement-on-progress-2-years-on. Last access: March 27, 2022.

CABINET OFFICE. **Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space.** London: The Stationery Office, 2009a. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf. Last access: March 27, 2022.

CABINET OFFICE. **National Security Capability Review**. 2018. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf. Last access: March 27, 2022.

CABINET OFFICE. **National Security Strategy and Strategic Defence and Security Review 2015**: First Annual Report 2016**.** 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/575378/national_security_strategy_strategic_defence_security_review_annual_report_2016.pdf. Last access: March 27, 2022.

CABINET OFFICE. **National Security Strategy and Strategic Defence and Security Review 2015:** Third Annual Report. 2019. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819613/NSS_and_SDSR_2015_Third_Annual_Report_-_FINAL__2_.pdf. Last access: March 27, 2022.

CABINET OFFICE. **Progress against the Objectives of the National Cyber Security Strategy**. 2012b. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/265401/Cyber_Security_Strategy_one_year_on_achievements.pdf. Last access: March 27, 2022.

CABINET OFFICE. **Progress against the Objectives of the National Cyber Security Strategy**. 2013b. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/265384/Progress_Against_the_Objectives_of_the_National_Cyber_Security_Strategy_December_2013.pdf. Last access: March 27, 2022.

CABINET OFFICE. **The National Cyber Security Strategy Our Forward Plans.** 2013a. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/265386/The_National_Cyber_Security_Strategy_Our_Forward_Plans_December_2013.pdf. Last access: March 27, 2022.

CABINET OFFICE. **The National Security Strategy of the United Kingdom**: Security in an interdependent world. London: The Stationery Office, 2008. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228539/7291.pdf. Last access: March 27, 2022.

CABINET OFFICE. **The National Security Strategy of the United Kingdom**: Update 2009 -Security for the Next Generation. London: The Stationery Office, 2009b. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/229001/7590.pdf. Last access: March 27, 2022.

CABINET OFFICE. **The UK Cyber Security Strategy:** Report on Progress and Forward Plans. 2014. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf. Last access: March 27, 2022.

CABINET OFFICE. **The UK Cyber Security Strategy- Report on progress:** Forward Plans. 2012a. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/265402/Cyber_Security_Strategy_Forward_Plans_3-Dec-12_1.pdf. Last access: March 27, 2022.

CABINET OFFICE. **The UK Cyber Security Strategy:** Protecting and promoting the UK in a digital world. London: Cabinet Office, 2011. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf. Last access: March 27, 2022.

CABIROL, Michel. La lutte informatique offensive n'est pas un tabou (Jean-Yves Le Drian). **La Tribune Fr.** 28 September 2015. Available at: https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/la-lutte-informatique-offensive-n-est-pas-un-tabou-jean-yves-le-drian-508269.html . Last access : May 22, 2022.

CAMBON, Christian. **Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020.** Assemblée nationale: Sénat, 2020. Available at: http://www.senat.fr/rap/r19-506/r19-5061.pdf . Last access: 22 May 2022.

CAMPUS CYBER. **Concept**. 2022. Available at: https://campuscyber.fr/. Last access: 9 May 2022.

CARR, Madeline. **US Power and the Internet in International Relations:** the irony of the information age. Hampshire: Palgrave, 2016.

CARRÈRE, Jean-Louis. **Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2011.** Assemblée nationale: Sénat, 2012. Available at: http://www.senat.fr/rap/r11-672/r11-6721.pdf . Last access: 22 May 2022.

CAVELTY, Miriam Dunn. Europe's cyber-power. **European Politics and Society**, v. 19 n. 3, 2018, pp.304-320 DOI: 10.1080/23745118.2018.1430718.

CENTER FOR FOR STRATEGIC AND INTERNATIONAL STUDIES - CSIS. **Significant Cyber Incidents Since 2006**. 2022. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/220404_Significant_Cyber_Incidents.pdf?6baqc92oMg0w.0wCwZLP6OATs9MmMmLG. Last access: March 27, 2022.

CERT.FR **A propos du CERT.FR**. 2022. Available at: https://www.cert.ssi.gouv.fr/a-propos/ Last access: May 9, 2022.

CHAOS COMPUTER CLUB - CCC. **Home**. Available at: https://www.ccc.de/en/home. Last access: June 20, 2022.

CHIERICI, Lorenzo.; FIORINI, Gian Luigi.; ROVERE, Stefano la.; VESTRUCCI, Paolo. The Evolution of Defense in Depth Approach: A Cross Sectorial Analysis. **Open Journal of Safety Science and Technology,** v. 6, n. 2, 8 September 2016, pp.35-54. DOI: 10.4236/ojsst.2016.62004.

COLEMAN, Nick. **Protecting Government Information:** Independent Review of Government Information Assurance – The Coleman report. 2008. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60967/ia_review.pdf. Last access: March 27, 2022.

COLLIN, Barry. Future of cyberterrorism: The Physical and Virtual Worlds Converge. **Crime and Justice International**. v. 2 n. 13, March 1997, p. 15-18. Available at: https://www.ncjrs.gov/App/publications/abstract.aspx?ID=171868. Last access: March 27, 2022

COSTA, Ricardo da Gama R. Introdução: Gramsci e a socialização da política. **Cadernos do ICP nº 1**, 2012. Available at: https://dariodasilva.wordpress.com/2012/11/30/antonio-gramsci-e-o-conceito-de-hegemonia1/. Last access: January 18, 2019.

COUNCIL OF EUROPE - COE. **Chart of signatures and ratifications of Treaty 185.** 2022 Available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185. Last access: March 27, 2022.

COUNCIL OF THE EU. **EU imposes the first ever sanctions against cyber-attacks**.30 July 2020. Available at: https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.Last access: June 20, 2022.

CYBER CERCLE. **Interview du député Christophe GUILLOTEAU sur le Pacte Défense Cyber**. Paris. 3 September 2015. Available at: https://cybercercle.com/interview-guilloteau-pacte-defense-cyber/. Last access: May 22, 2022.

CYMUTTA, Sebastian. **National Cybersecurity Organisation:** GERMANY [National Cybersecurity Governance Series]. Tallinn: NATO CCDCOE, 2020. Available at: https://ccdcoe.org/uploads/2020/12/Country_Report_DEU.pdf . Last access: June 21, 2022.

DAHL, Robert. A. A Critique of the Ruling Elite Model. **American Political Science Review,** v. 52, n. 2, 1958. pp. 463-469. DOI: 10.2307/1952327.

DAHL, Robert. A. The Concept of Power. **Behavioral Science**, v. 2, n. 3, 1957. p. 201- 215.

DARWISH, Amber.; ROMANIUK, Scott N. Cybersecurity in the French Republic. *In:* ROMANIUK, Scott N.; MANJIKIAN, Mary (eds). **Routledge Comparison to Global Cybersecurity Strategy,** London/New York: Routledge, 2021. p. 62-72.

DATA GUIDANCE. **UK:** NIS Regulations 2021 come into force, incident reporting threshold is lowered. 18 January 2022. Available at: https://www.dataguidance.com/news/uk-nis-regulations-2021-come-force-incident-reporting. Last access: March 27, 2022.

DEAN, Mitchell. Power as Sumbolon: Sovereignty, Governmentality and the International. *In:* BENDITTI, Philippe.; BIGO, Didier.; GROS, Frederic (eds). **Foucault and the Modern International Silences and Legacies for the Study of World Politics**, New York: Palgrave Macmillan US, 2017.

DÉFENSE ET SÉCURITÉ NATIONALE. **Le Livre Blanc.** Paris: Odile Jacob and La Documentation Française, 2008. Available at: https://www.vie-publique.fr/sites/default/files/rapport/pdf/084000341.pdf . Last access: May 9, 2022.

DELLA PORTA, Donatella.; KEATING, Michael. How many approaches in the social sciences? Na epistemological introduction. *In:* DELLA Porta, Donatella.; KEATING, Michael (eds). **Approaches and Methodologies in the Social Sciences** -a Pluralist Perspective**.** Cambridge: Cambridge University Press, 2008. pp.19-39

DELLA PORTA, Donatella.; KEATING, Michael. Comparative analysis: case-oriented versus variable-oriented research *In*: DELLA Porta, Donatella.; KEATING, Michael (eds). **Ap-**

proaches and Methodologies in the Social Sciences - a Pluralist Perspective, Cambridge: Cambridge University Press, 2008. Pp198-222

DEMCHAK, Chris C. Cybered Conflict, Hybrid War, and Informatization wars. *In:* TIKK, Eneken.; KERTTUNEN, Mika (eds). **Routledge Handbook of International Cybersecurity**. New York: Routledge, 2020 pp.36-51, E-Book Kindle.

DENNISON, Susi.; FRANKE, Ulrike Esther.; ZERKA, Pawel**. The Nightmare of the dark: the security fears that keep Europeans awake at night**. 2018. Available at: https://ecfr.eu/special/the_nightmare_of_the_dark_the_security_fears_that_keep_europeans_awake_at_n/#:~:text=European%20Power-,The%20nightmare%20of%20the%20dark%3A%20The%20security%20fears%20that%20keep,cyber%20attacks%20to%20climate%20change. Last access: October 24, 2019.

DESFORGES, Alix.; GÉRY, Aude. France Doesn’t Do Public Attribution of Cyberattacks. But It Gets Close. **LAWFARE** [Blog]. September 3, 2021. Available at: https://www.lawfareblog.com/france-doesnt-do-public-attribution-cyberattacks-it-gets-close Last access: July 02, 2022.

DESFORGES, Alix. **Approche géopolitique du cyberespace:** les enjeux pour la défense et la sécurité nationale: l'exemple de la France. 2018. PhD Thesis.École Doctorale des Sciences Sociales (Vincennes/Saint-denis). Université Paris 8. Paris, 2018.

DEUTSCHE WELLE - DW. **Data stolen during hack attack on German parliament, Berlin says**. 29 May 2015. Available at: https://www.dw.com/en/data-stolen-during-hack-attack-on-german-parliament-berlin-says/a-18486900. Last access: June 21, 2022.

DEUTSCHER BUNDESTAG. **Parlamentarisches Kontrollgremium (PKGr).** 2022a. Available at: https://www.bundestag.de/ausschuesse/weitere_gremien/parlamentarisches_kontrollgremium Last access: June 21, 2022.

DEUTSCHER BUNDESTAG. **Plenarprotokoll 17/74.** 24 November 2010. Available at: https://dserver.bundestag.de/btp/17/17074.pdf . Last access: August 13, 2022.

DEUTSCHER BUNDESTAG. **Plenarprotokoll 18/16** - Stenografischer Bericht. 19. Februar 2014. Available at: https://dserver.bundestag.de/btp/18/18016.pdf . Last access: June 21,2022.

DEUTSCHER BUNDESTAG. **Schlußbericht der Enquete-Kommission Zukunft der Medien in Wirtschaft und Gesellschaft.** Deutschlands Weg in die Informationsgesellschaft* zum Thema Deutschlands Weg in die Informationsgesellschaft. Drucksache 13/1 1004. Bonn: Bonner Universitäts-Buchdruckerei. 22 June 1998. Available at: https://dserver.bundestag.de/btd/13/110/1311004.pdf . Last access: June 20, 2022.

DEUTSCHER BUNDESTAG. **Unterrichtung durch das Parlamentarische Kontrollgremium** Bericht über die Kontrolltätigkeit gemäß § 13 des Gesetzes über die parlamentarische Kontrolle nachrichtendienstlicher (Berichtszeitraum November 2013 bis November 2015). Drucksache 18/7962. 21 March 2016. Available at: https://dserver.bundestag.de/btd/20/003/2000310.pdf . Last access: June 21, 2022.

DEUTSCHER BUNDESTAG. **Unterrichtung durch die Bundesregierung** Bericht der Bundesregierung zum Stand der Bemühungen um Rüstungskontrolle, Abrüstung und Nichtverbreitung sowie über die Entwicklung der Streitkräftepotenziale (Jahresabrüstungsbericht 2021). Drucksache 20/1657. 28 April 2022b. Available at: https://dserver.bundestag.de/btd/20/016/2001657.pdf . Last access: June 21, 2022.

DEUTSCHER BUNDESTAG. **Unterrichtung durch das Parlamentarische Kontrollgremium** Bericht über die Kontrolltätigkeit gemäß § 13 des Gesetzes über die parlamentarische Kontrolle nachrichtendienstlicher (Berichtszeitraum Dezember 2015 bis Oktober 2017). Drucksache 19/422. 15 January 2018. Available at: https://dserver.bundestag.de/btd/19/004/1900422.pdf . Last access: June 21, 2022.

DOBSON, Melina.; DYMYDIUK, Jason.; MAINWARING, Sarah. Operation Rubicon: the most successful intelligence heist of the 20th Century. **Warwick Knowledge Center**. 2020. Available at: https://warwick.ac.uk/newsandevents/knowledgecentre/society/politics/operation_rubicon/ Last access: July 02, 2022.

DPA. Germany reveals offensive cyberwarfare capability. **Atlantic Council**. June 8, 2012. Available at: https://www.atlanticcouncil.org/blogs/natosource/germany-reveals-offensive-cyberwarfare-capability/. Last access: June 20, 2022.

DUCARU, Sorin. NATO advances in its new operational domain: cyberspace. **Fifth Domain** July 5, 2018. Available at: https://www.fifthdomain.com/opinion/2018/07/05/nato-advances-in-its-new-operational-domain-cyberspace/. Last access: March 26, 2019.

DUFFIELD, John.S. **World Power Forsaken. Political Culture, International Institutions, and German Security Policy After Unification,** Stanford, CA: Stanford University Press, 1998

ECONOMIC AND RESEARCH COUNCIL - ESCR. **Prevent UK's Counter-Terrorism Strategy** (Social Science for Schools). Available at: https://esrc.ukri.org/public-engagement/social-science-for-schools/resources/prevent-the-uk-s-counter-terrorism-strategy/ Last access: March 27, 2022.

EGLOFF, Florian J. **Semi-State Actors in Cyberspace**. New York: Oxford University Press, 2022.

ENLOE, C. Margins, Silences, and Bottom Rungs: How to overcome the underestimation of power in the study of International Relations. *In:* SMITH, Steven.; BOOTH, Ken.; ZALEWSKI, Marysia. **International Theory:** positivism and beyond. Cambridge University Press, 1996. p. 186-203.

ERB, Scott. **German Foreign Policy. Navigating a New Era, Boulder.** Boulder: Lynne Rienner, 2003.

EUROPEAN COMMISSION. **Digital Economy and Society Index (DESI) 2020 France**. Brussels: 2020a.

EUROPEAN COMMISSION. **Digital Economy and Society Index (DESI) 2020 Germany.** Brussels: 2020b.

EUROPEAN COMMISSION. **Digital Economy and Society Index (DESI) 2020 United Kingdom**. Brussels: 2020c.

EUROPEAN COMMISSION. **Digital Economy and Society Index (DESI) 2021 France**. Brussels: 2021

EUROPEAN COMMISSION. **Digital Economy and Society Index (DESI) 2021 Germany.** Brussels: 2021.

EUROPEAN COMMISSION. **Questions and Answers:** Digital Economy and Society Index (DESI) 2021. Brussels, 12 November 2021b. Available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_5483. Last access: July 13, 2022.

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY - ENISA. **France Country Report.** January 2010. Available at: https://joinup.ec.europa.eu/sites/default/files/document/2014-12/France%20Country%20Report.pdf. Last access: May 9, 2022.

FEDERAL MINISTRY OF INTERIOR. **Cyber Security Strategy for Germany**. Berlin: BMI, February 2011.

FEDERAL MINISTRY OF THE INTERIOR, BUILDING, AND COMMUNITY - BMI. **Cyber Security Strategy for Germany 2021**. Berlin: BMI, August 2021. Available at: https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf;jsessionid=761B0EC92F5FC3F7DC7481A2D08C0CDF.2_cid364?__blob=publicationFile&v=4. Last access: June 21, 2022.

FEDERAL OFFICE FOR INFORMATION SECURITY - BSI. **The IT Security situation in Germany in 2007**. Bonn: Federal Office for Information Security, April 2007. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2007.pdf?__blob=publicationFile&v=1.Last access: May 27, 2022.

FEDERAL OFFICE FOR INFORMATION SECURITY - BSI. **The IT Security situation in Germany in 2009**. Bonn: Federal Office for Information Security, January 2009. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2009.pdf?__blob=publicationFile&v=1. Last access: May 27, 2022.

FEDERAL OFFICE FOR INFORMATION SECURITY - BSI. **The IT Security situation in Germany in 2014**. Bonn: Federal Office for Information Security, November 2014. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?__blob=publicationFile&v=1. Last access: June 21, 2022.

FEDERAL OFFICE FOR INFORMATION SECURITY - BSI. **The IT Security situation in Germany in 2015**. Bonn: Federal Office for Information Security, November 2015. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2015.pdf?__blob=publicationFile&v=2. Last access: June 21, 2022.

FEDERAL OFFICE FOR INFORMATION SECURITY - BSI. **The IT Security situation in Germany in 2017**. Bonn: Federal Office for Information Security, August 2017. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2017.pdf?__blob=publicationFile&v=1. Last access: June 21, 2022.

FEDERAL OFFICE FOR INFORMATION SECURITY - BSI. **The IT Security situation in Germany in 2018**. Bonn: Federal Office for Information Security, September 2018. Available at:https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2018.pdf?__blob=publicationFile&v=1. Last access: June 21, 2022.

FEDERAL OFFICE FOR INFORMATION SECURITY (BSI). **The IT Security situation in Germany in 2019**. Bonn: The Federal Office for Information Security. October 2019. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2019.pdf?__blob=publicationFile&v=1. Last access: June 21, 2022.

FEDERAL OFFICE FOR INFORMATION SECURITY - BSI. **The IT Security situation in Germany in 2020**. Bonn: Federal Office for Information Security, September 2020. Available at:https://www.hannovermesse.de/apollo/hannover_messe_2021/obs/Binary/A1087894/201210_BSI_Lagebericht_2020_EN.pdf. Last access: June 21, 2022.

FEDERAL OFFICE FOR INFORMATION SECURITY (BSI). **The IT Security situation in Germany in 2021**. Bonn: Federal Office for Information Security, September 2021. Available at:https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2021.pdf?__blob=publicationFile&v=5. Last access: June 21, 2022.

FEMIA, Joseph. V. **Gramsci's Political Thought**: Hegemony, Consciousness, and the Revolutionary Process. Oxfor: Calendon press, 1987.

FERREIRINHA, Isabella M. N.; RAIZ, Tânia R. As relações de poder em Michel Foucault: reflexões teóricas. **Revista de Administração Pública (RAP).** Rio de Janeiro, v. 44, n. 2, 2010. pp. 367-83.

FLEMING, Jeremy. **Director GCHQ's Speech at CYBERUK 2019**. 24 April 2019b. Available at: https://www.gchq.gov.uk/pdfs/speech/director-s-speech-at-cyberuk-2019.pdf Last access: March 27, 2022.

FLEMING, Jeremy. **Director's speech on Cyber Power** – as delivered. 29 March 2019a. Available at: https://www.gchq.gov.uk/pdfs/speech/jeremy-fleming-fullerton-speech-singapore-2019.pdf. Last access: March 27, 2022.

FOREIGN AND COMMON OFFICE - FCO; HAGUE, William. **London Conference on Cyberspace:** Chair's statement, 2011. Available at: https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement. Last access: March 27, 2022.

FOREIGN, COMMONWEALTH & DEVELOPMENT OFFICE - FCDO. **UK sanctions relating to cyber activity**. 18 June 2020. Available at: https://www.gov.uk/government/collections/uk-cyber-sanctions. Last access: March 27, 2022.

FOUCAULT, Michel. **Discipline and Punish: The Birth of the Prison,** transl. Alan Sheridan, New York: Vintage Books, 1979.

FRANCE DIPLOMACY. **Elysée Treaty**. 2022. Available at: https://www.diplomatie.gouv.fr/en/country-files/germany/france-and-germany/elysee-treaty/. Last access: May 9, 2022.

FRANCE DIPLOMATIE. La mission de l’Ambassadeur pour le numérique. 2022. Available at: https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-mission-de-l-ambassadeur-pour-le-numerique/ .Last access: May 23, 2022.

GAIA-X. **About Gaia-X**. 2022. Available at: https://gaia-x.eu/what-is-gaia-x/about-gaia-x/ Last access: July 20, 2022.

GATEAU, Christine and FARON, Pauline. French law for a Digital Republic: what you should know, what you should expect. **Lexology.** 2016. Available at: https://www.lexology.com/library/detail.aspx?g=d2f9a06a-bd26-4a7a-9594-0ae639d51bd1 Last access: May 9, 2022.

GAVENTA, J. Levels, Spaces and forms of power: analysing opportunities for change. **IDS Bulletin,** v. 37, n. 6, 2006.

GILPIN, Robert. **War and Change in World Politics.** Cambridge: Cambridge University Press, 1981.

GOMEZ, Miguel Alberto. Identifying Cyber Strategies vis-a-vis Cyber Power. **2013 World Cyberspace Cooperation Summit IV (WCC4),** Palo Alto, CA, 2013, pp. 1-7. DOI: 10.1109/WCS.2013.7050504.

GONZALEZ, Wenceslao J. Lakatos’s approach on prediction and novel facts. **Theoria:** An International Journal for Theory, History, and Foundations of Science, v. 16, n. 3, 2001, pp. 499–518. Available at: http://www.jstor.org/stable/23918415.Last access: August 24, 2022.

GREENWALD, Glenn.; MACASKILL, Ewen. NSA Prism program taps into user data of Apple, Google and others. **The Guardian,** 07 June 2013. Available at: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. Last access: March 27, 2022.

GOUVERNMENT. **Cybersécurité, faire face à la menace: la estratégie française**. 18 February 2021. Available at: https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=2A6148DF-BF21-4A64-BDF8-79BACE2AE255&filename=686%20-DP%20cyber.pdf . Last access: May 23, 2022.

GOUVERNMENT. **Le Programme d'investissements d'avenir**. 2028. Available at: https://www.gouvernement.fr/le-programme-d-investissements-d-avenir. Last access: October 24, 2021.

GOVERNMENT COMMUNICATIONS HEADQUARTERS - GCHQ. **National Cyber Force transforms country's cyber capabilities to protect the UK**. 19 November 2020. Available at: https://www.gchq.gov.uk/news/national-cyber-force?adhoc_referrer=041603018002. Last access: March 27, 2022.

GRAY, Colin S. **Making strategic sense of cyber power:** Why the sky is not falling. Carlisle: Strategic Studies Institute and U.S. Army War College Press, 2013.

GRIGSBY, Alex. The End of Cyber Norms. **Survival,** v. 59, n. 6, 2017. p. 109-122. DOI: 10.1080/00396338.2017.1399730.

GUZZINI, Stefano. Marx Weber's Power. *In:* Lebow, Richard N. **Max Weber and International Relation**s Cambridge: Cambridge University Press, 2017. pp. 97-118.

GUZZINI, Stefano. **Power, Realism and Constructivism**. New York: Routledge, 2013.

HAASTER, Jelle van. Assessing Cyber Power. *In:* PISSANIDIS, N.; RÕIGAS, H.; VEENENDAAL, M. **8th International Conference on Cyber Conflict:** Cyber Power, Tallinn: NATO CCD COE Publications, 2016, p. 7-22.

HARE, Forrest. The cyber threat to national security: Why we can't agree, *In:* **Conference on Cyber Conflict Proceedings 2010**, 2010, pp. 211–225.

HAYWARD, Clarissa.; LUKES, Steven. Nobody to shoot? Power, structure, and agency: A dialogue. **Journal of Power**, v. 1, n. 1, p. 5 - 20, 2008. DOI: 10.1080/17540290801943364

HELEN, Jon.; SOLON, Olivia. 'Petya' ransomware attack strikes companies across Europe and US. **The Guardian (online).** 27 June 2017. Available at: https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe. Last access: March 27, 2022.

HER MAJESTY GOVERNMENT - HMG. **Strong Britain in an Age of Uncertainty:** The National Security Strategy. London: The Stationery Office, 2010a. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf. Last access: March 27, 2022.

HER MAJESTY GOVERNMENT - HMG. **Global Britain in a competitive age:** The Integrated Review of Security, Defence, Development and Foreign Policy. 2021a. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/

file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf Last access: March 27, 2022.

HER MAJESTY GOVERNMENT - HMG. **National Cyber Security Strategy 2016-2021.** 2016. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf. Last access: March 27, 2022.

HER MAJESTY GOVERNMENT - HMG. **National Cyber Strategy 2022:** Pioneering a cyber future with the whole of the UK. 2021b. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf. Last access: March 27, 2022.

HER MAJESTY GOVERNMENT - HMG. **National Security Strategy and Strategic Defence and Security Review 2015**. London: Williams Lea Group, 2015. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478936/52309_Cm_9161_NSS_SD_Review_PRINT_only.pdf. Last access: March 27, 2022.

HER MAJESTY GOVERNMENT - HMG. **Securing Britain in an Age of Uncertainty:** The Strategic Defence and Security Review. London: The Stationery Office, 2010b. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf. Last access: March 27, 2022.

HERN, Alex. WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017. **The Guardian (online).** 30 December 2017. Available at: https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware. Last access: March 27, 2022.

HERPIG, Sven.; HEUMANN, Stefan. Germany's Crypto Past and Hacking Future. **Lawfare**. 13 April 2017. Available at: https://www.lawfareblog.com/germanys-crypto-past-and-hacking-future. Last access: May 25, 2022.

HERPIG, Sven.; MORGUS, Robert.; SHENIAK, Amit. Active Cyber Defense - A Comparative Study on US, Israeli and German Approaches. **Konrad Adenauer Stiftung**, 2020. Available at:https://www.kas.de/documents/263458/263507/Active+Cyber+Defense+-+A+comparative+study+on+US,+Israeli+and+German+approaches.pdf. Last access: June 21, 2022.

HOLLIS, Martin.; STEVE Smith. **Explaining and Understanding International Relations.** Clarendon Press, 1991.

HOME OFFICE. **Serious Crime Act 2015 Fact sheet:** Part 2: Computer misuse. 2015. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415953/Factsheet_-_Computer_Misuse_-_Act.pdf. Last access: March 27, 2022.

HOPF, Ted. **The Promise of Constructivism in International Relations Theory**. International Security, v. 23, n. 1, 1998, pp. 171-200.

HORENBEECK, Maarten Van. **FIRST at the Global Conference on Cyberspace (GCCS)**. 2018. Available at: https://www.first.org/blog/20180106-FIRST_at_the_GCCS. Last access: March 27, 2022.

HOUSE OF COMMONS. **Cyber-attack on the NHS** (Thirty-Second Report of Session 2017–19). 18 April 2018. Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/787/787.pdf. Last access: March 27, 2022.

HUTTON, John. **Strategy for Transformational Government Enabled by Technology:** Cabinet Office written statement. 02 November 2005 (c43WS). Available at: https://www.theyworkforyou.com/wms/?id=2005-11-02b.43WS.1. Last access: March 27, 2022.

INFORMATION COMMISSIONER’S OFFICE. **About the DPA 2018**. 2022. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-dpa-2018/about-the-dpa-2018/#2. Last access: March 27, 2022.

INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT - ISC. **Annual Report 2012-2013**. London: The Stationery Office, 2013b. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/211553/31176_HC_547_ISC.PDF. Last access: March 27, 2022.

INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT - ISC. **Annual Report 2013-2014.** London: Williams Lea Group, 2014. Available at: https://isc.independent.gov.uk/wp-content/uploads/2021/01/2013-2014_ISC_AR.pdf. Last access: March 27, 2022.

INTELLIGENCE AND SECURITY COMMITTEE - ISC. **Annual Report 2007-2008**. London: The Stationery Office, 2009. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61300/gov_response0708.pdf. Last access: March 27, 2022.

INTELLIGENCE AND SECURITY COMMITTEE - ISC. **Annual Report 2008-2009.** London: The Stationery Office, 2010. Available at: https://isc.independent.gov.uk/wp-content/uploads/2021/01/2008-2009_ISC_AR.pdf. Last access: March 27, 2022.

INTELLIGENCE AND SECURITY COMMITTEE - ISC. **Annual Report 2009-2010**. London: The Stationery Office, 2010. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61295/isc-annualreport0910.pdf. Last access: March 27, 2022

INTELLIGENCE AND SECURITY COMMITTEE - ISC. **Annual Report 2010-2011**. London: The Stationery Office, 2011. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/211561/isc-annualreport1011.pdf. Last access: March 27, 2022

INTELLIGENCE AND SECURITY COMMITTEE - ISC. **Annual Report 2011-2012**. London: The Stationery Office, 2012. Available at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/211559/ISC-2011-12.pdf. Last access: March 27, 2022

INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT - ISC. **Annual Report 2015-2016**, London: Williams Lea Group, 2016. Available at: https://isc.independent.gov.uk/wp-content/uploads/2021/01/2015-2016_ISC_AR.pdf. Last access: March 27, 2022

INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT - ISC. **Annual Report 2016-2017,** London: APS Group, 2017. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727949/ISC-Annual-Report-2016-17.pdf. Last access: March 27, 2022

INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT - ISC. **Annual Report 2019-2021**. Fetcham, Leatherhead: HH Associates Ltd, 2021. Available at: https://isc.independent.gov.uk/wp-content/uploads/2021/12/ISC-Annual-Report-2019%E2%80%932021.pdf. Last access: March 27, 2022

INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT - ISC. **Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme,** 2013a. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/225459/ISC-Statement-on-GCHQ.pdf. Last access: March 27, 2022

INTELLIGENCE SECURITY COMMITTEE OF PARLIAMENT - ISC. **Annual Report 2017-2018**. London: APS Group, 2018. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/772726/HC1692_ISC_Annual_Report_2017_18.pdf. Last access: March 27, 2022.

INTELLIGENCE SECURITY COMMITTEE OF PARLIAMENT - ISC. **Privacy and Security: A modern and transparent legal framework,** London: Williams Lea Group, 2015. Available at: https://www.pdpjournals.com/docs/88433.pdf. Last access: March 27, 2022

INTERNATIONAL COMMITTEE OF THE RED CROSS - ICRC. **What are jus ad bellum and jus in bello?** Available at: https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0. Last access: May 9, 2022.

INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES - IISS. **Cyber Capabilities and national power:** A Net Assessment, 2021. Available at: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power. Last access: May 9, 2022.

INTERNATIONAL TELECOMMUNICATIONS UNION - ITU. **Global Cyber Index 2017. 2017.** Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. Last access: March 26, 2019.

INTERVIEWEE A. **Interview 1** [August 2020]. Interviewer: Bruna Toso de Alcântara 1 .mp3 file (50 min.).

INTERVIEWEE B. **Interview 2** [September 2020]. Interviewer: Bruna Toso de Alcântara.

INTERVIEWEE C. **Interview 3** [September 2020]. Interviewer: Bruna Toso de Alcântara 2.mp3 file (78 min.).

INTERVIEWEE D. **Interview 4** [June 2020]. Interviewer: Bruna Toso de Alcântara 3.mp3 file (39 min.).

INTERVIEWEE E. **Interview 5** [August 2020]. Interviewer: Bruna Toso de Alcântara.

INTERVIEWEE F. **Interview 6** [August 2020]. Interviewer: Bruna Toso de Alcântara.

JACKSON, Patrick Thadeus. **The conduct of inquiry in International Relations**: philosophy of science and its implications for the study of world politics. London: Routledge, 2010.

JORDAN, Tim. **Cyberpower:** the culture and politics of cyberspace and the internet. New York: Routledge, 1999.

JOUBERT, Vincent. Dossier d'actualité: La cybersécurité et la cyberdéfense en question. **Fondation pour la Recherche Stratégie**.10 February 2014. Available at: https://www.frstrategie.org/publications/autres/dossiers/cybersecurite-cyberdefense-question-2014 . Last access : May 22, 2022.

JOYCE, Daniel. Privacy in the Digital Era: Human Rights Online? **Melbourne Journal of International Law**, v. 16 issue 1**.** 2015. Available at: https://law.unimelb.edu.au/__data/assets/pdf_file/0003/1586811/16109Joyce2.pdf. Last access: June 20, 2020.

KAPLAN, Morton A. The New Great Debate: Traditionalism vs. Science in International Relations. **World Politics**, v. 19, n. 1, 1966. pp. 1-20.

KATZENSTEIN, Peter. J.; SEYBERT, Lucia A. Protean Power and Control Power: Conceptual Analysis. *In:* KATZENSTEIN, Peter. J.; SEYBERT, Lucia A (eds) **Protean Power: Exploring the Uncertain and Unexpected in World Politics.** New York: Cambridge University Press, 2018, pp. 2-25, E-Book Kindle

KLIMBURG, Alexander. Mobilising Cyber Power, Survival: Global. **Politics and Strategy**, v. 53 n.1, February-March 2011, pp. 41-60, DOI: 10.1080/00396338.2011.555595.

KLIMBURG, Alexandre.; FAESEN, Louk. A Balance of Power in cyberspace. *In:* BROEDERS, Dennis.; VAN DER BERG, Bibi. **Governing Cyberspace:** Behavior, Power and Diplomacy. London: Rowman & Littlefield, 2020 pp. 145-172, E-Book Kindle

KNOX, Benjamin J. The Effect of Cyberpower on Institutional Development in Norway. **Frontier in Psychology**. v. 9 n.717, 2018. DOI: 10.3389/fpsyg.2018.00717

KUEHL, Daniel. From Cyberspace to Cyberpower: Defining the Problem. *In:* KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K. **Cyberpower, and National Security**. Washington Dc: Potomac Books Inc., 2009. pp. 24-42.

LAMONT, Christopher. **Research Methods in International Relations**. SAGE Publications, 2015.

LANGO, Hans-Inge. Competing Academic Approaches to Cybersecurity. *In:* FRIIS, Karsten; RINGSMOSE, Jens. **Conflict in Cyber Space Theoretical, Strategic and Legal Perspectives.** New York: Routledge, 2016.

LASBORDES, Pierre. **La sécurité des systèmes d'information:** un enjeu majeur pour la France. Paris: La Documentation française, 2006. Available at: https://www.vie-publique.fr/rapport/27943-la-securite-des-systemes-dinformation-un-enjeu-majeur-pour-la-france. Last access: May 23, 2022.

LAUDRAIN, Arthur P. B. France's New Offensive Cyber Doctrine. **Lawfare.** February 26, 2019b. Available at: https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine.Last access: May 23, 2022.

LAUDRAIN, Arthur P. B. The State, its Institutions and Processes: Applying Decision-Making Models to French Cyber Security and Defence. 2019a. **International Studies Association (ISA) Annual Conference 2020**. Available at: SSRN: https://ssrn.com/abstract=3432338 or http://dx.doi.org/10.2139/ssrn.3432338. Last access May 23, 2022.

LÉGIFRANCE. **LOI n. 2016-1321 du 7 octobre 2016 pour une République numérique** – Exposé des Motifs. 2022. Available at: https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000031589829/?detailType=EXPOSE_MOTIFS&detailId . Last access: 22 May 2022.

LIBICKI, Martin C. **Cyberspace in Peace and War** [Second Edition]. Annapolis: Naval Institute Press, 2021.

LIBICKI, Martin. C. **Conquest in cyberspace:** national security and information warfare. Cambridge: Cambridge University Press, 2007.

LIVRE BLANC SUR LA DÉFENSE. **Le Livre Blanc Sur la Défense.** Paris: La Documentation Française, 1994. Available at: https://www.vie-publique.fr/sites/default/files/rapport/pdf/944048700.pdf . Last access : May 9, 2022.

LONERGAN, Shawn William. **Cyber Power and the International System.** Doctor Thesis (Philosophy) - Graduate School of Arts and Sciences, Columbia University, New York, 2017.

LUKES, Steven. Power and the Battle for Hearts and Minds. **Millennium-Journal of International Studies**, v. 33, n.3, 2005a. pp. 477-493.

LUKES, Steven. **Power a Radical View.** New York: Palgrave, 2005b.

MANJIKIAN, Mary. **Introduction to Cyber Politics and Policy.** Washington DC: Sage Publications, 2021. E-Book Kindle.

MAURER, Tim. **Cyber Mercenaries:** The State, Hackers, and Power. New York: Cambridge University Press, 2018.

MCCARTHY, Daniel R. **Power, Information Technology, and International Relations Theory**: The Power and Politics of US Foreign Policy and Internet. Hampshire: Palgrave, 2015.

MCCARTHY, Thomas David. **Traveling Domain Theory:** A Comparative Approach for Cyberspace Theory Development. 2012. Thesis (Doctor of Philosophy) – Faculty of The Fletcher School of Law and Diplomacy, Medford.

MIDDLETON, Bruce. **A History of Cyber Security Attacks:** 1980 to present. New York: Auerbach Publications, 2017.

MILLER, Greg. The intelligence coup of the century' For decades, the CIA read the encrypted communications of allies and adversaries. **Washington Post.** Feb 11, 2020. Available at: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/. Last access: July 02, 2022.

MINGST, Karen A.; ARREGUÍN-TOFT, Ivan M. **Essentials of International Relations.** 7th Edition. New York: W. W. Norton & Company, 2017.

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR DE LA RECHERCHE ET DE L'INNOVATION (MESRI). **Déclaration d'intention conjointe formalisant les liens entre les réseaux français et allemands en Intelligence Artificielle, 2020.** Available at: https://www.enseignementsup-recherche.gouv.fr/fr/declaration-d-intention-conjointe-formalisant-les-liens-entre-les-reseaux-francais-et-allemands-en-49019 .Last access: July 20, 2022.

MINISTÉRE DE LA DÈFENSE. **French White Paper on Defence and National Security, 2013.** Tulle: Pôle graphique de Tulle. 2013. Available at: http://www.livreblancdefenseetsecurite.gouv.fr/pdf/the_white_paper_defence_2013.pdf . Last access: May 22, 2022.

MINISTÉRE DE LA DÈFENSE. **Pacte Défense Cyber:** 50 mesures pour changer d'échelle, 2014. Available at: https://www.gwendal-rouillard.fr/wp-content/uploads/2015/01/pacte_de_fense_cyber-1.pdf . Last access: May 22, 2022.

MINISTÈRE DES ARMÉES. **Politique ministérielle de lutte informatique défensive.** Paris: DICoD Bureau des Éditions. 2019a. Available at: https://www.defense.gouv.fr/sites/default/files/ministere-armees/Politique%20minist%C3%A9rielle%20de%20lutte%20informatique%20d%C3%A9fensive.pdf . Last access : May 23, 2022.

MINISTÈRE DES ARMÉES. **Éléments publics de doctrine militaire de lutte informatique offensive**. Paris: DICoD / Pôle éditions, 2019b. Available at: http://lignesdedefense.blogs.ouest-france.fr/files/E%CC%81le%CC%81ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20offensive%20%20.pdf . Last access: May 23, 2022.

MINISTÈRE DES ARMÉES. **Droit International Appliqué aux Operations dans le Cyberspace**. Paris, 2019c. Available at: https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf . Last access: May 23, 2022.

MINISTÈRE DES ARMÉES. **Strategic Update 2021**. Paris: DICoD Bureau des Éditions, January 2021a. Available at: https://www.stjornarradid.is/library/03-Verkefni/Almannaoryggi/Thjodaroryggismal/France%20-%20Strategic%20Review%202021.pdf . Last access: May 23, 2022.

MINISTRY OF DEFENCE (MoD) **Cyber primer.** 2014. Available at: https://www.gov.uk/government/publications/cyber-primer. Last access: March 27, 2022.

MINISTRY OF DEFENCE (MoD). **Digital Strategy for Defence:** Delivering the Digital Backbone and unleashing the power of Defence's data. April 2021. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/990114/20210421_-_MOD_Digital_Strategy_-_Update_-_Final.pdf. Last access: March 27, 2022.

MORGUS, Robert *et al.* "Are China and Russia on the Cyber Offensive in Latin America and the Caribbean? A Review of Their Cyber Capabilities and Implications for the U.S. and its Partners in the Region". **New America**. July 2019. Available at: https://d1y8sb8igg2f8e.cloudfront.net/documents/Are_China_and_Russia_on_the_Cyber_Offensive_in_Latin_America_and_the_Caribbean_final.pdf. Last access: March 23, 2022.

MUELLER, Milton. **Will the Internet Fragment?** Sovereignty, Globalization, and Cyberspace. Cambridge: Polity Press, 2017.

NATIONAL AUDIT OFFICE - NAO. **The UK cyber security strategy:** Landscape review. London: The Stationery Office, 2013. Available at: https://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf. Last access: March 02, 2022.

NATIONAL CRIME AGENCY - NCA. **Introduction to the Computer Misuse Act 1990**. Available at: https://www.nationalcrimeagency.gov.uk/who-we-are/publications/523-cyber-choices-hacking-it-legal-computer-misuse-act-1990/file. Last access: March 27, 2022.

NETZPOLITIK. **Geheime Cyber-Leitlinie:** Verteidigungsministerium erlaubt Bundeswehr Cyberwar und offensive digitale Angriffe. 30 July 2015. Available at: https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/#:~:text=Geheime%20Cyber%2DLeitlinie%20Verteidigungsministerium%20erlaubt,%E2%80%9Eoffensiven%20Cyber%2DF%C3%A4higkeiten%E2%80%9C . Last access: June 21, 2022.

NORTH ATLANTIC TREATY ORGANIZATION - NATO. **Cyber Defence Pledge**. 8 July 2016. Available at: https://www.nato.int/cps/en/natohq/official_texts_133177.htm. Last access: May 9, 2022.

NYE, Joseph S. Junior. **Cyberpower.** Harvard Kennedy School, 2010. Available at: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf. Last access: September 30, 2016.

NYE, Joseph S. Junior. **The Future of Power**. New York: Public Affairs, 2011.

NYE, Joseph. S. Junior. Soft Power. **Foreign Policy**, v. 80, 1990. pp. 153-171. DOI: https://doi.org/10.2307/1148580

OFFICE FOR NATIONAL STATISTICS - ONS. **UK Digital Economy Research:** 2019. 28 January 2022. Available at: file:///C:/Users/Bruna%20T/Downloads/UK%20Digital%20Economy%20Research_%202019.pdf. Last access: July 13, 2022.

OLADIMEJI, Saheed.; KERNER, Sean M. **SolarWinds hack explained:** Everything you need to know. 16 June 2021. Available at: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know. Last access: June 21, 2022.

PARIS CALL. **The 9 Principles.** 2022. Available at: https://pariscall.international/en/principles.Last access: May 9, 2022.

POULIOT, Vincent. Practice Tracing. *In:* BENNETT, Andrew.; CKECKLE, Jeffrey. T. **Process Tracing:** From Metaphor to Analytic Tool. Cambridge: Cambridge University, 2015.

PREMIER MINISTRE. **French national digital security strategy.** Paris, 2015. Available at: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf. Last access: May 22, 2022.

PROUST, Oliver. France Adopts Digital Republic Law. **Fildfisher**. 4 October 2016. Available at: https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/france-adopts-digital-republic-law. Last access: May 9, 2022.

PUGLIERIN, Jana.; FRANKE, Ulrike Esther. The Big engine that might: how France and Germany can build a Geopolitical Europe**. ECFR [Policy Brief]**. July 2020. Available at: https://ecfr.eu/wp-content/uploads/the_big_engine_that_might_how_france_and_germany.pdf Last access: July 17, 2022).

RAFFARIN, Jean-Pierre.; URVOAS, Jean-Jacques **Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014.** Assemblée nationale: Sénat, 2014. Available at: https://www.assemblee-nationale.fr/14/pdf/rap-off/i2482.pdf . Last access: May22, 2022).

RAGIN, Charles. **The Comparative Method:** moving beyond qualitative and quantitative strategies.Oakland: University of California Press, 1987.

RATTRAY, Gregory J. An Environmental Approach to Understanding Cyberpower. *In:* KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K (org.). **Cyberpower and National Security.** Washington Dc: Potomac Books Inc., 2009. pp. 253-274.

REINHOLD, Thomas.; REUTER, Christian. From Cyber war to Cyber Peace. *In:* REUTER, Christian. **Information Technology for Peace and Security:** IT applications and infrastructures in conflicts, crises, war, and peace. Wiesbaden: Springer Vieweg, 2019.

REPUBLIQUE FRANÇAISE. **Defence and National Security Strategic Review 2017.** Paris; DICo Bureau des éditions, 2017. Available at: https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/DEFENCE%20AND%20NATIONAL%20SECURITY%20STRATEGIC%20REVIEW%202017.pdf. Last access: May 23, 2022.

REPUBLIQUE FRANÇAISE. **Journal officiel "Lois et Décrets" (JORF) n° 0294 du 19 décembre 2013**. 19 December 2013. Available at: https://www.legifrance.gouv.fr/download/pdf?id=GGbH9qmFDXehzGSyi9SFw59zMW9r0VCLrkV8AmAAT3o= . Last access: May 23, 2022.

RITTBERG, Volker. **German Foreign Policy Since Unification**: Theories and Case Studies. Manchester: Manchester University Press, 2001.

ROMANI, Roger. **Rapport D´Information. Sénat – Session extraordinaire de 2007-2008**. Annexe au procès-verbal de la séance du 8 juillet 2008. Au nom de la commission des Affaires étrangères, de la défense et des forces armées (1) sur la cyberdéfense. Strasbourg, France. Available at: https://www.senat.fr/rap/r07-449/r07-4491.pdf . Last access: May 9, 2022.

ROMANIUCK, Scott N.; CLAUS, Michel. Germany’s Cybersecurity Strategy: Confronting future challenges. *In:* ROMANIUCK, Scott N.; MANJIKIAN, Mary. **Routledge Companion to Global Cyber-Security Strategy**. London: Routledge, 2021. pp.73-88.

ROWLAND, JILL.; RICE, MASON.; SHENOI, SUJEET. The anatomy of a cyber power. **International Journal of Critical Infrastructure Protection**, v. 7, n. 1, 2014. pp. 3-11.

SCHALLBRUCH, Martin.; SKIERKA, Isabel. **Cybersecurity in Germany:**. Cham: Springer International Publishing AG, 2018. **(**SpringerBriefs in Cybersecurity series)

SCHMITT, Michael. The United Kingdom on International Law in Cyberspace**. EJIL: Talk!** 24 May 2022. Available at: https://www.ejiltalk.org/the-united-kingdom-on-international-law-in-cyberspace/. Last access: July 20, 2022.

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET LA SÉCURITÉ NATIONALE - SGDSN. **Revue stratégique de cyberdéfense.** 12 February 2018b. Available at: http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf .Last access : May 23, 2022.

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET LA SÉCURITÉ NATIONALE - SGDSN. **Strategic review of cyber defence.** 12 February 2018a. Available at: http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf .Last access: May 23, 2022.

SEGAL, Adam. **The Hacked World Order:** How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age, New York: Public Affairs, 2016.

SEKINE, Daisuke. Review of From Mahan to Corbett? **The Sawasaka Peace Foundation.** February 2012. Available at: https://www.spf.org/oceans/analysis_en/c1202.html. Last access: May 23, 2022.

SEMPA. Francis P. The Geopolitical Vision of Alfred Thayer Mahan. **The Diplomat** (online) December 30, 2014. Available at: https://thediplomat.com/2014/12/the-geopolitical-vision-of-alfred-thayer-mahan/.Last access: May 23, 2022.

SHAKARIAN, Paulo.; SHAKARIAN, Jana.; RUEF, Andrew. **Introduction to Cyber-Warfare:** a Multidisciplinary Approach. Masachuttes: Elsevier, 2013.

SHELDON, John B. Toward a Theory of Cyber Power: Strategic Purpose in Peace and War. *In:* REVERON, Derek S. **Cyberspace, and National Security:** threats opportunities in a virtual world. Washington DC: Georgetown University Press, 2012. p. 207-224.

SIEDSCHLAG, Alexander. Germany: From a reluctant power to a constructive power? *In:* KIRCHNER, Emil J.; SPERLING, James. **Global Security:** Governance Competing perceptions of security in the 21st century. New York: Routledge, 2007.

SINGH, J. P. Meta-power, Networks, Security and Commerce. *In:* CAVELTY, Miriam Dunn.; MAUER, Victor.; KRISHNA-HENSEL, Sai Felicia. **Power and Security in the Information Age**: Investigating the Role of the State in Cyberspace, Hampshire: Ashgate Publishing Limited, 2007. pp. 45-66

SPARK, Laura S.; MULLEN, Jethro. France summons U.S. ambassador after reports U.S. spied on presidents. **CNN**. June 24, 2015. Available at: https://edition.cnn.com/2015/06/24/europe/france-wikileaks-nsa-spying-claims/index.html Last access: July 02, 2022.

SPIEGEL I**nside Snowden's Germany File**. 18 June 2014. Available at: https://www.spiegel.de/international/germany/new-snowden-revelations-on-nsa-spying-in-germany-a-975441.html. Last access: June 20, 2022.

SPIEGEL. **WannaCry- Attacke – Fakten zum globalen Cyberangriff**. 13 May 2017. Available at: https://www.spiegel.de/netzwelt/web/wannacry-attacke-fakten-zum-globalen-cyber-angriff-a-1147523.html . Last access: June 21, 2022.

STARR, Stuart H. Towards an Evolving Theory of Cyberpower. *In:* CZOSSECK, Christian.; GEERS, Kenneth. **The Virtual Battlefield: Perspectives on Cyber Warfare**. Amsterdam: IOS Press. Cryptology and Information Security Series Volume 3, 2009, p. 18–52. Available at: http://www.ebooks.iospress.com/volumearticle/27608. Last access: January 21, 2019.

STEIGER, Stefan. **Cybersicherheit in Innen- und- Außenpolitik:** deutsche und britische policies im vergleich. Bielefeld: Transcript Verlag, 2022. E Book Kindle.

STERLING-FOLKER, J. & SHINKO, R. E. Discourses of Power: traversing the realist-postmodern divide. **Millennium** v..33, n., p. 637-664, 2005.

STEVENS, Tim. United Kingdom: Pragmatism and adaptability in the cyber realm *In:* ROMANIUK, Scott N.; MANJIKIAN, Mary. **Routledge Comparison to Global Cyber-Security Strategy,** London/New York: Routledge, 2021a. p.191- 200.

STEVENS, Tim. **Brexit and Beyond:** Cyber Security. 2021b. Available at: https://www.kcl.ac.uk/cyber-security-brexit-and-beyond. Last access: March 27, 2022.

STRATÉGIE INTERNATIONALE DE LA FRANCE POUR LE NUMÉRIQUE. Paris. December 2017. Available at: https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf . Last access: May 23, 2022.

SUEUR, Jean-Pierre. **Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2013.** Assemblée nationale: Sénat, 2014. Available at: http://www.senat.fr/rap/r13-462/r13-4621.pdf . Last access : May 22, 2022.

SUEUR, Jean-Pierre.; ADAM, Patricia. **Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2012.** Assemblée nationale: Sénat, 2013. Available at: http://www.senat.fr/rap/r12-557/r12-5571.pdf . Last access: May 22, 2022.

TABANSKY, Lior. Towards a Theory of Cyber Power: The Israeli Experience with Innovation and Strategy. *In:* PISSANIDIS, N.; RÕIGAS, H.; VEENENDAAL, M. **8th International Conference on Cyber Conflict:** Cyber Power, Tallinn: NATO CCD COE Publications, 2016, p. 51-64.

TECHNOLOGY STRATEGY BOARD. **Our strategy for 'Digital Britain.'** 2009. Available at: https://www.bl.uk/britishlibrary/~/media/bl/global/business-and-management/pdfs/non-secure/o/u/r/our-strategy-for-digital-britain.pdf. Last access: March 27, 2022.

THE FEDERAL GOVERNMENT. **Digital Agenda 2014 – 2017**. München: Federal Ministry for Economic Affairs and Energy, Federal Ministry of the Interior, Federal Ministry of Transport and Digital Infrastructure, August 2014. Available at: https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2014/digital-agenda.pdf?__blob=publicationFile&v=2. Last access: June 21, 2022.

THE FEDERAL GOVERNMENT. **On the Application of International Law in Cyberspace** [Position Paper]. March 2021. Available at: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf. Last access: June 21, 2022.

THE FEDERAL GOVERNMENT. **White Paper 2016 on German Security Policy and the Future of the Bundeswehr**. Berlin: Federal Ministry of Defence, June 2016. Available at: https://issat.dcaf.ch/download/111704/2027268/2016%20White%20Paper.pdf. Last access: June 21, 2022.

TIDEY, Alice. EU sanctions two Russian military officers over cyber attack against German parliament. **Euronews.** 23 October 2020. Available at: https://www.euronews.com/my-europe/2020/10/23/eu-sanctions-two-russian-military-officers-over-cyber-attack-against-german-parliament. Last access: June 21, 2022.

TILLY, Charles. **Big structures, large processes, huge comparisons.** New York: Russel Sage Fdtn., 1984.

UK GOV. **Counter-terrorism strategy (CONTEST).** 12th July 2011. Available at: https://www.gov.uk/government/publications/counter-terrorism-strategy-contest. Last access: March 27, 2022.

UK GOVERNMENT. **Joint Intelligence Organisation**. 2022. Available at: https://www.gov.uk/government/groups/joint-intelligence-organisation. Last access: March 27, 2022.

UK PARLIAMENT. **The intelligence services and the Snowden revelations.** 2022. Available at: https://www.parliament.uk/business/publications/research/key-issues-parliament-2015/defence-and-security/intelligence-services/. Last access: March 27, 2022.

UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND - UK. **United Nations Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security** – Application of International Law to Sates Conduct in Cyberspace – United Kingdom Statement. 2021. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/990851/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.pdf. Last access: July 20, 2022.

UNITED NATIONS - UN. **Developments in the field of information and telecommunications in the context of international security, 2022.** Available at: https://www.un.org/disarmament/ict-security/. Last access: August 13, 2022.

VALERIANO, Brando.; MANESS, Ryan C. **Cyber War versus Cyber Realities**: Cyber Conflict in the International System. Oxford: Oxford University Press, 2015.

VALERIANO, Brandon.; JENSEN, Benjamin.; MANESS, Ryan C. **Cyber Strategy:** the evolving character of power and coercion. Oxford: Oxford University Press, 2018.

VIE PUBLIQUE. **Déclaration de M. Jean-Yves Le Drian, ministre de la défense, sur la cyberdéfense, à Bruz le 12 décembre 2016.** 12 December 2016. Available at: https://www.vie-publique.fr/discours/201492-declaration-de-m-jean-yves-le-drian-ministre-de-la-defense-sur-la-cyb. Last access: May 9, 2022.

VIE PUBLIQUE. **Déclaration de Mme Florence Parly, ministre des armées, sur le volet de la cyberdéfense des armées, à Paris le 18 janvier 2019.** 18 January 2019. Available at: https://www.vie-publique.fr/discours/269137-florence-parly-18012019-strategie-cyber-des-armees-cyberdefense. Last access: May 9, 2022

VITEL, Philippe.; BLIDDAL, Henrik. French Cyber Security and Defence: An Overview. **Information & Security**: An International Journal**,** v. 32, n. 1, 2015. pp. 29-41. Available at: https://isij.eu/system/files/3209_france.pdf. Last access: May 22, 2022).

VOO, Julia *et al*. National Cyber Power Index 2020 – Methodological and Analytical Considerations. China Cyber Policy Initiative (Report). **Belfer Center for Science and International Affairs** at Harvard Kennedy School**.** September 2020. Available at: https://www.belfercenter.org/publication/national-cyber-power-index-2020. Last access: May 22, 2022

WALTZ, Edward. **Information Warfare:** principles and operations**.** Boston, Artech House: 1998.

WARSMANN, Jean-Luc.; ROHAN, Josselin de. **Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2010.** Assemblée nationale: Sénat, 2010. Available at: http://www.senat.fr/rap/r10-188/r10-1881.pdf . Last access: May 22, 2022.

WEBBER, Douglas. **New Europe, New Germany, Old Foreign Policy?** german foreign policy since unification. London: Cass, 2001.

WEBER, Max. **Wirtschaft und Gesellschaft:** Grundriß der Verstehenden Soziologie. 5. Auflage. Tübingen: J. C. B. Mohr/Paul Siebeck, 1980. Available at: https://books.google.de/books?id=RWK_6TKVENcC&printsec=frontcover&hl=de#v=onepage&q&f=false . Last access: May 22, 2022.

WENDT, Alexander. **Social Theory of International Politics.** Cambridge: Cambridge University Press, 1999.

WENDT, Alexander. Anarchy is What States Make of It: the social construction of power politics. **International Organization,** v. 46, n. 2, 1992.

WIGHT, Colin. Philosophy of Social Science and International Relations. *In*: CARLSNAES, W.; RISSE-KAPPEN, T.; SIMMONS, BA. **Handbook of International Relations**. London: Sage Publications Inc., 2013, pp. 29-56.

WILLSHER, Kim.; HELEY. Jon. Emmanuel Macron's campaign hacked on eve of French election. **The Guardian**. 6 May 2017. Available at: https://www.theguardian.com/world/2017/may/06/emmanuel-macron-targeted-by-hackers-on-eve-of-french-election. Last access: May 9, 2022.

WUNDERLICH, Carmen. **Rouge States as Norm Entrepreneurs:** black sheep or sheep in wolve's clothing? Cham: Springer Nature Switzerland, 2020.

XUETONG, Yan. Bipolar Rivalry in the Early Digital Age. **The Chinese Journal of International Politics**, v. 13, n. 3, 2020. p. 313–341. DOI: https://doi.org/10.1093/cjip/poaa007

YORK, Dan. What Is the Splinternet? And Why You Should Be Paying Attention. **Internet Society Blog**. 23 March 2022. Available at: https://www.internetsociety.org/blog/2022/03/what-is-the-splinternet-and-why-you-should-be-paying-attention/. Last access: August 11, 2022.

APPENDIX A – SEMI-STRUCTURED INTERVIEW

This is the questionnaire as part of the research "A Comparative study on Cyber Power: The United Kingdom, France and Germany" developed by the researcher Bruna Toso de Alcântara. The following questions shall be answered freely, having in mind a broad concept of cyberspace, encompassing information systems (hardware and software) and the human users that interact with them.

1. How do you see interactions in cyberspace? Do they involve power relations? Among which actors?

2. How do you see cyber actors' capacity for achieving power in cyberspace? Would it be easier for one of them to gain cyber power? Why?

3. What elements do you believe would be necessary to constitute "cyber power"?

4. How do you see having and projecting cyber power? Are they the same thing?

5. What would be, in your opinion, feasible ways for a state to project cyber power? For instance: using cyber proxies, cyber diplomacy, export national emerging technologies…

6. How do you see the relationship between cyber power and national power (political, diplomatic, economic, and military)? Would these powers be detached from each other?

7. How do you see the relationship between cyber power and states' position in the international system? For instance: Would this relationship exist? What format would it take (hierarchical/horizontal)? Would it justify states acting strategically in cyberspace?

8. How do you think offensive and defensive capabilities affect cyber power? Would one of them be preferable over the other? Why?

9. What elements do you consider essential for a state to maintain cyber power? How would you prioritize them?

10. How would you rank your country scaling from 1 to 10, being 1 with no cyber power at all and ten as a cyber-superpower, both internationally and regionally? Justify your score.