IMSISS
International Master
Security, Intelligence
& Strategic Studies

Erasmus
Mundus

# The Rise of Net-States in the Cyberspace:

## Cyber Power Dynamics and the Disruption of International Security

**July 2023**

**UoG: 2652576V**
**DCU: 21109265**
**CU: 13871785**

**Presented in partial fulfilment of the requirements for the Degree of International Master in Security, Intelligence and Strategic Studies**

**Word Count:** 21,177
**Supervisor:** Dr Tomáš Kučera
**Date of Submission:** 28th July 2023

University of Glasgow
DCU
UNIVERSITY OF TRENTO
CHARLES UNIVERSITY

# Table of Contents

# Acknowledgements

《Hopes and Dreams》

*"Live to learn and*
*learn to live*
*For which life is a journey*
*Where no end is ever meet"*

*To those whom I am most devoted to, thank you for being there for me in this long journey.*
*To my colleagues, to the new people I met, to the places of inspiration, thank you.*
*To myself, thank you for believing, now keep dreaming, and living.*

# Introduction

## The 4th Industrial Revolution Age: The Physical and Cyber as One World

The pioneering Third Industrial Revolution or Digital Era was marked by significant technological developments that, since the last century, have led to the digitalisation of several industries. The introduction of computer and electronic systems and the Internet automated manufacturing processes and production, resulting in the creation of new economic markets and modern means of communication (Schwab, 2015). Now, as the world progressively transitions into the age of the Fourth Industrial Revolution, the next wave of technological innovations will transform human mankind as never seen before. Current technologies such as robotics, Internet of Things (IoT), blockchain, autonomous vehicles, 3D printing and, more recently, artificial intelligence and quantum computing, are driving future trends that have large disruptive potential across several sectors and industries (McKinsey, 2022). Thus, as these innovations continue to revolution modern global societies, present scholarly paradigms on how humans experience the world must be re-evaluated.

To represent this shift, the concept of 4th Industrial Revolution (4IR) was introduced – symbolising the convergence among the physical, digital and biological realms (Schwab, 2023). As witnessed in recent years, technological devices and digital platforms have become an intrinsic part of everyday life – improving people's quality of life and work performance. However, what distinguishes the 4IR from the previous era is the exponential rate at which these emergent technologies are transforming life in all aspects at all levels. Driven primarily by cyber-physical systems, advanced analytics and connectivity; this revolutionary era is characterised by three main elements – velocity, scope and complexity. Advocates of the 4IR argue that the speed at which technological innovations are being employed and combined is drastically altering entire systems of production, management and governance (Schwab, 2015). In addition, the vast amount of information generated from the implementation of previous information technologies has reached unprecedented levels recorded in history – referred to as Big Data. With events such as the Covid-19 pandemic accelerating these changes by throwing the world into a digital frenzy (Ross & Maynard, 2021).

Moreover, built upon the widespread availability of digital technologies and increased internet accessibility, this 4IR is creating a global world in which human-machine interconnectivity takes a new meaning. On one hand, innovative breakthroughs occurring simultaneously in sectors including private, public and academia are propelling cooperation through real-time exchange of data at a global level. For instance, the increased use of IoT in industries and homes means a higher interconnectivity between systems and people. On the other, digital mediums in the form of social media networks have massively improved people's social interactions which are starting to integrate the newest technologies such as AI (Ross & Maynard, 2021). Therefore, the breadth and depth of systemic changes brought by the 4IR is further developing complex, dynamic and interconnected ecosystems. A fusion of smart systems that integrate with organisations and people is envisioned as the core ideal guiding future technology – closing the gap between the physical and digital (Schwab, 2023). Hence, as human-machine interactions keep developing and strengthening, the effects and impacts that humans produce in the real world will have an influence on the digital and vice versa. Blurring the boundaries between these dimensions to be considered as one.

However, with the abundant opportunities that come with the era of the 4IR, the implications of this digital integration into the physical world "will be guided by the choices that people make today" (Schwab, 2023, p. 2). Historical records have demonstrated that, much like in previous revolutions, technological innovation had critical repercussions for the international system (Eden, 2018). Therefore, for states, this implies an urgent reassessment of policymaking and decision-making in general – as modern societies across the world presently undergo the initial phases of this 4IR. For instance, some countries have started to incorporate this concept into their policies reflecting the importance of acknowledging the opportunities and challenges of emergent technology (Clark, 2019; Yang & Gu, 2021). Particularly in the development of regulatory frameworks that would contribute to anticipate, prepare and respond to changes caused by the increasingly integration of these technologies. However, recognising the 4IR massive influence in shaping the future is not enough as governments struggle to keep up with the pace of technological innovations.

In fact, the growing number and reliance on emergent technologies to provide solutions and basic services in several settings is becoming difficult to regulate – at least from a top-down approach (Yang & Gu, 2021). The legacy of the digital revolution, apart from making life simpler, has brought forward new emergent risks in the form of cyber-attacks, misinformation and cybercrime. In addition, 4IR acceleration of innovation and scope for disruption has augmented vulnerabilities and uncertainties at the national and international levels. Repercussions such as dynamic and unpredictable economic markets, greater civic movements and demands for rights, and shifts in power of nations are all happening at once (Schwab, 2015). Hence, the complexity of networked cyber-physical systems and human manipulation of technology for a positive —or negative —purpose means that more than ever, challenges faced by nation states are multiplying exponentially.

Among these challenges, the maintenance of national interests and security is proving to be a top priority in political agendas for governments around the world (Yang & Gu, 2021). Technological and human progress had profound effects in shaping the nature of international security i.e., peace and conflicts (Schwab, 2015). And so far, this 4IR is following this formula as the use of innovative technology in warfare is being visible in modern conflicts. For example, the recent war of Russian against Ukraine has demonstrated combating skills that were ‘hybrid’ in nature, combining cyber capabilities with traditional battlefield techniques. Therefore, the possibility for future conflict scenarios in which actions taken at the physical level affect the cyber domain and vice versa are expected to become more common. Consequently, the potential demands from crises occurring simultaneously in these realms suggest that nation states must start "to think strategically about the forces of disruption and innovation shaping our future" (Schwab, 2017, p. 3). Thus, by acting today policymakers can ensure a positive 4IR progression, guiding the world towards the beneficial evolution of mankind.

## The Present Study

To develop "a comprehensive and globally shared view of how technology is affecting our lives and reshaping our economic, social, cultural, and human environments" (Schwab, 2015, p. 6), it is crucial to understand the application of traditional international relations to the cyber realm. Through this dissertation, therefore, I am seeking to address which major non-state actors, empowered by the cyberspace, could disrupt the present international security landscape. Principally, it will examine the power, influence and strategical implication of prevailing cyber entities hereinafter defined as Net States by expanding on existing theories and concepts. Net States are a relatively new and rapidly evolving phenomenon that challenges traditional notions of governance and sovereignty. Hence, understanding their activities, motivations, and impact is important for developing better security strategies. This might involve monitoring Net state activities, the creation of international norms and standards or new legal frameworks for addressing digital disruption. To provide greater clarity about the function and structure of cyberspace to policymakers, security professionals and other stakeholders.

### Aim and objectives

The overall purpose of this dissertation is to contribute on the knowledge about the cyber and physical co-evolution process our world is currently undergoing. It intends to explore the role of Net States and thereby state actors in cyberspace – a largely ignored topic by scholars within the fields of international relations and security studies (Choucri and Clark, 2019). Much of the previous research on the issue of non-state actors in cyberspace has been conducted from a militarised or legal framework perspective (Bussolati, 2015). Focusing almost exclusively on states extension of power into the cyber domain for its control, management and strategical operation. Thus, to achieve the stated purpose, this dissertation will be driven by two main objectives:

1. To assess the concept of Net States as a novel phenomenon outside the traditional framework of state-to-state relations that governs international security. How they are structured and the ways in which operate and influence the cyberspace – political systems and socio-economic structures.

2. To analyse Net States' potential disruption on international security and cyber power from a global geopolitical and strategical context. The creation of dependencies and security vulnerabilities between traditional nation states and Net states that could lead to conflict or cooperation within the cyberspace.

Studying Net States would bring insights into how digital technologies are changing traditional conceptions of security, the identification of challenges for internet governance and international relations sovereignty.

## Research questions

Guiding this dissertation are the following research questions: (a) What are Net States and how do they exercise direct control and influence in cyberspace? Are Net States empowered by the inherent cyberspace structure? (b) Does the rise of Net States direct transformational change in cyberspace? What impact do they have on the perception of international security?

## Methodology

To answer these questions in accordance with the objectives proposed, the present dissertation uses a qualitative research methodology. Based on an abduction approach, it is further divided into two main parts – the inductive and deductive.

For the first part pertaining to the conceptual elaboration of Net States, case studies are employed to uncover the principal characteristics and functions of Net States. The chosen cases involve the well recorded events of Big Tech during the Trump administration, Anonymous and WikiLeaks. Through the empirical research of preexisting conceptual ideas, this dissertation will attempt to develop a preliminary model to act as a basis for further theoretical development and insights.

For the second part, international security and cyber power dynamics, a few cases (between 2020-2022) are scrutinised in an analogous manner to the study conducted by Gamero-Garrido (2014). Each case is individually examined to determine the different entities involved, power relations and their outcomes. By performing content analysis, it will measure the interactions between Net states and traditional states to compare power balance, and the possibility of contention or cooperation. A hypothesis will be formulated based on previous findings from the first part to draw an inference on whether Net States do pose a significant threat to the international security landscape.

Sources for the different cases presented in this dissertation are mainly based on secondary data and materials from various sources, drawing examples that cover non-state actors and state actors.

## Dissertation Overview

After a brief introduction into the dissertation’s aim, objectives, research questions and methodology; the remaining chapters proceed as the following:

The next chapter will delve into current literature on the intricacies between the digital (cyberspace) and the physical (international relations). It will review (i) what the cyberspace entails as a domain and infrastructure, and (ii) the cyber security dilemma within cyberspace. Hence, the contextual nature of cyberspace will be deconstructed from a technological and social perspective.

Building on the literature review, the third chapter will revisit the key principles and theoretical framework of Neorealism while discussing the emergent phenomenon of Net States. Introducing these cyber entities as a concept parallel to the state unit level of analysis which exists in our physical world. Within this chapter, this dissertation will examine whether Net States might stand as a model for new forms of cyber structures in cyberspace.

The fourth chapter will provide a deeper understanding of the cyber power dynamics and the disruptive consequences for the international system. Views on internet governance and cyber power relations among major nation states will be discussed. In this section, a hypothesis formulated from previous literature discussion will evaluate Net States strategical presence in cyberspace.

In the final chapter, findings from the dissertation will be discussed – expanding on the theoretical and strategical consequences of Net States for international security. Limitations encountered throughout the analytical process would be considered and thoughts for future research will be suggested. Final conclusions will be drawn as closing remarks in regard to this dissertation’s contribution to the overall existing literature.

# Literature Review

## The Cyberspace: Internet and Connectivity

As a revolutionary global phenomenon, the conception of a ‘alternative’ cyber reality has transcended the boundaries of the ‘real’ physical world in which, we, as human beings coexist. This alternative virtual reality, broadly referred to as cyberspace, is frequently used as an umbrella term to describe the complex techno-social ecosystem upon which is constructed. Originated in science fiction to illustrate an immersive electronic environment where artificially intelligent beings inhabit (Gibson, 1984), modern cyberspace rather reflects the information space of societies emulating the physical world (Barlow 1996). A unique interdependent network system of infrastructures consisting of the Internet, telecommunications networks and computer systems operated and shaped by humans. In literature, the meaning of ‘cyberspace’, nevertheless, remains a disputed topic with little consensus among stakeholders in the public, private sector and academia. For instance, as the Internet evolved allowing social and political discussions, cyberspace became of interest to nation states’ high-politics, converting it into a contested space (Bussell, 2013). Just recently, the North Atlantic Treaty Organisation (NATO) declared cyberspace an operational ‘domain’ along with traditional land, air, sea and outer space domains (Crowther, 2017). Hence, as a dynamic and developing concept integrating two different yet similar realities, it is essential to understand cyberspace from a cyber and international relations (IR) perspective. For this purpose, the following definition proposed by Choucri and Clark (2019, p. 3) will guide the overall narrative of this dissertation:

> Cyberspace: “(i) is built as a layered construct where physical elements enable a logical framework of interconnection; (ii) that permits the processing, manipulation, exploitation, augmentation of information, and the interaction of people and information; (iii) is enabled by institutional intermediation and organisation; and (iv) is characterized by decentralization and interplay among actors, constituencies, and interests.”

Another significant aspect of cyberspace as a conceptual medium is certain key characteristics that distinguishes it from other domains traditionally associated to the physical world. The most common being arguably the non-existent boundaries or territories (jurisdictions), which as a international phenomenon transcends the constraints of location and geography in the physical realm (Bussolati, 2015). As an artificial artefact of decentralised technological networks, the processing of information and human interactions occurs at a fluid rate in the sense of something existing everywhere and nowhere (Cavelty, 2015a). Moreover, this abstract network ecosystem can be composed of many alternative cyberspaces driven by different visions and principles at different layers; defined, constructed and created by different approaches to interconnection (Choucri and Clark, 2019). Therefore, from a IR perspective the absence of 'borders' represents a serious issue that impedes the establishment of sovereignty and norms applicable under international law (Johnson & Post, 1996). Although, what actually drives this complex nexus between technology and human interaction is the core infrastructure known as Internet.

The Internet, an invention present since its foundation in 1983, has been a key part in the digital revolution, globalising information and communications. Described as a 'network of networks', it is the backbone of the modern world and the most fundamental infrastructure that holds the majority of human and information interconnectivity (Bronk, 2012). Hence, the Internet does not have a central authority to control it, but rather is an aggregation of systems, protocols, standards, hardware and organisations that oversight its functioning (Knake, 2010; O'Hara & Hall, 2018). Among its components, it encompasses the Domain Name System (DNS) and the codes for exchanging data, the Internet Protocol (IP) which allocates addresses for communicating at a distance (Nye, 2010). Consequently, the structure of Internet has international standing, and at the same time, a global reach that has fostered new ways of bringing people together. Within this space of networks users are able to interact with each other and form communities, cutting across the physical boundaries with extremely low barriers (Perritt, 1998). Despite this, the Internet has exponentially evolved in the last years, being subject to even more rapid technological changes altering its infrastructure and governance (De Gregorio & Radu, 2022). This has brought new forms of economic, social and political conventions which have been integrated into modern societies much rapidly than the ability to appreciate their full implications. Thus, the Internet, as a collective global space, poses a higher risk for global contention due to the increased access of a new variety of actors with different interests to pursue and capabilities (Nye, 2010).

The ease by which people can participate in cyberspace, however, has complemented a proliferation of cyber actors and the promotion of a cyber culture that celebrates freedom (Perritt, 1998). In return, these cyber actors composed of individuals, groups and organisational entities such as businesses are shaping the cyberspace, particularly the Internet, simulating social structures on top of a networked technical system. Therefore, the malleable and complex nature of cyberspace hinders a tangible visualisation that could allow a better understanding of this immense abstract space that continues to evolve (O'Hara & Hall, 2018). In order to conceptualise cyberspace for a better understanding to IR, it is necessary to analyse the Internet as simple framework to trace its activity and principal cyber actors. For this purpose, Choucri and Clark (2019) developed an Internet model composed of different layers that portray the blending of cyberspace's physical and virtual properties (see Figure 1).

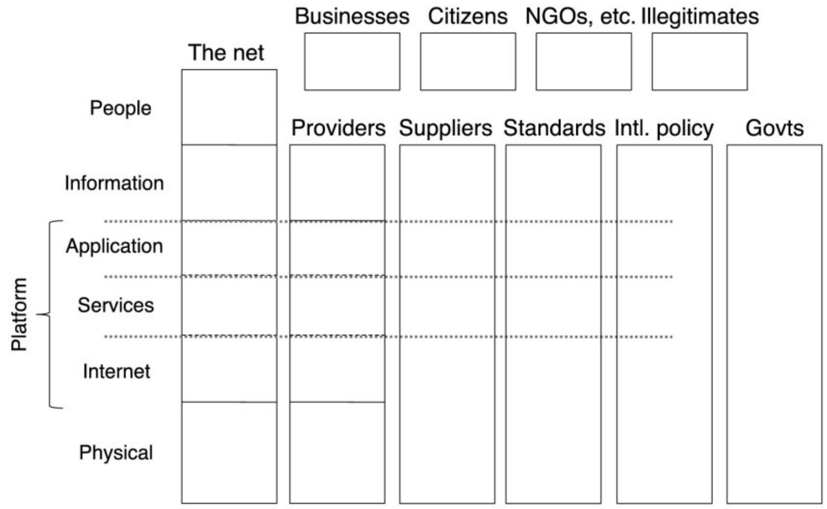

*Figure 1.* Layered model of Internet (vertically) including different types of actors (horizontally) and users of cyberspace (top). Adapted from "International Relations in the Cyber Age: The Co-Evolution Dilemma," by N. Choucri and D. D. Clark, 2019, p. 48.

This model is significant because it represents the core structure of Internet and the interconnection of actors and actions at various levels to analyse the distribution of power and interactions. From the top, the (a) people layer is the most dynamic, consisting of the users and constituencies who participate and shape cyberspace through the leverage of capabilities and demands for better functionality; (b) the next layer, information, consists of any type of information stored, transmitted and transformed in cyberspace; (c) the platform comprises the provision of services that builds on the physical components; and (d) finally, the physical layer that supports logical elements and represents the tangible and concrete manifestation of devices, servers and cables (Choucri and Clark, 2019). In this sense, this model can be interpreted as a point of entry to observe and analyse cyber actors, their behaviour, operations and structures. However, such model has been classically attributed to computer science field, therefore, the implications for IR remain limited. Nevertheless, the deconstruction of cyberspace into different layers could result useful to locate cyber actors and ultimately, understand security and governance in the cyber domain (Reardon & Choucri, 2012).

## Cyber security: The Dilemmas and Challenges

Cyberspace perpetration into the physical world is dictating a new normal in the form of digital disruption. Characterised by the diversification of actors and decentralised connectivity of multiple devices, digital disruption can impulse innovation or cause security concerns in cyberspace (Tonhauser & Ristvej, 2019). In a positive sense, digital disruption invites new actors with fewer economic resources to successfully leverage digital technology to create better price-performance value businesses or solutions. This creates a surge in digital platforms or market communities that might led to the gradual substitution of tradition industries in the physical world. For instance, the popular digital platform Airbnb has disrupted the sector of hospitality, offering peer-to-peer short term accommodation or experiences worldwide (Rosenstand, Gertsen, & Vesti, 2018). Echoing the "move fast and break things" ethos of technological firms in declaration to a newly formed digital world order in cyberspace (Net Politics, 2020). Digital inventions like these that show growing demand from an Internet user base are causing the progression of traditional industries such as health, banking and retail to move into the cyberspace (Faesen, Torossian, Mayhew, & Zensus, 2020). However, industries transition into this domain, as well, as citizens becoming used to their digital lives in this medium pose security challenges for states.

This is where the negative connotation of disruption is implemented, which refers to the identification of elements in cyberspace that are easy for exploitation acts by malicious actors (Tonhauser & Ristvej, 2019). This type of disruption has greater implications for the economy, politics and society of states as barriers of entry are very low and the availability of cyber tools is increasing (Nye, 2022). For instance, cyber security reports about data breaches tend to show increasing costs as activities such as cybercrime becomes more lucrative (Shull & Hilt, 2021). Likewise, the market dynamics of disruption has allowed an industry to emerge from exploiting and finding vulnerabilities, for example companies offering cyber security, as well as DarkWeb market sales of cyber tools (Schmidt & Cohen, 2010). Hence, this poses a critical challenge for the national security of states as cyber-attacks against critical infrastructure is expected to keep rising in the future. As the evolution and emergence of new cyber threats continues at a fast pace, states, nevertheless, must learn to adapt to rapid changes in cyberspace through cyber resilience practices (Tonhauser & Ristvej, 2019). As history has shown, societies take time to respond to major technological disruptions, and now cyberspace are making those even more complex (Nye, 2022). In addition, misinformation and influence operations are modern digital issues embedded in cyberspace that can jeopardise states' sovereignty. For example, in states with democratic regimes, the fundamental values are based on informed citizens who have access to facts to make political decisions (Wexler & Oberlander, 2023). As consequence, disinformation or influential operations can distort information about reality endangering public trust in governance by causing polarity.

Disruptive or persistent cyber-attacks, moreover, can test population's trust in the governance and authority of states in delivering security, which can further cause erosion of sovereignty (Wexler & Oberlander, 2023). Meanwhile, states' expansion of activities into the cyberspace means that for them the issue of ensuring cyber security is intrinsically related to their national purposes and interests. As the costs of applying a set of mechanisms on some non-state actors could actually benefit other actors in a common pursuit for better security. States, therefore, have concentrated on domestic cyber security measures to defend themselves from cyber threats, becoming a priority at the expense of international cooperation (Choucri and Clark, 2019). From this perspective, the securitisation of cyberspace is relegated to the technological components most vulnerable to cyber-attacks which have sufficient physical association to a state's territory (Mueller, 2020).

In an ideal world, the most desired outcome, however, would be to achieve a global cyber security that ensures the complete protection of the cyberspace. From its physical technical roots all the way to the more abstract information and people's layers through revolutionary technology or a combination of practices, norms and technology. A utopian hypothetical scenario based on a defence structure with very limited grounds for malicious operations (Healey, 2011). However, the volatile nature and unique characteristics of the cyberspace hinders this possibility because a virtuous cyber security as the end goal is “aspirational, not actionable” (Choucri and Clark, 2019, p. 59). Therefore, to achieve better means of security, it is necessary to break this grandiose goal into smaller and actionable objectives.

A resolution proposed to address this issue has been a whole-of-nation approach, which refers to the collaboration between governments and a diverse range of actors involving private sector, academia and other civil organisations. This approach has been traditionally implemented in conflict areas to support peace and stability by achieving common goals, which in cyberspace would provide resilience against evolving and sophisticated security threats (Doyle, 2019). Because the cyberspace is diverse and multi-layered, accounting for all cyber-attacks perpetrated at the different levels would be inefficient for states alone. Hence, collaboration and cooperation with influential non-state actors are crucial in the development and prevention of conflicts (Klimburg, 2011b). For this reason, many states in their cyber security strategies have emphasised the importance of integrating into their objectives a whole-of-nation approach to limit competitive behaviour and ensure better security in cyberspace (Luiijf, Besseling, Spoelstra, & de Graaf, 2013). However, actions described to achieve this objective are yet to be put into practice by states, intensified by the increase of non-states actors engaged in the stabilisation of cyberspace (Doyle, 2019). Thus, the management of the cyberspace dominated by contention rather than cooperation remains as a dilemma for the international community (Choucri and Clark, 2019).

For a long time, cyber security has been understood as the protection of information from cyber threats performed through computing and communication technologies, very much aligned with information security (Azmi, Tibben, & Win, 2016). However, as illustrated above, the implications of cyber threats and challenges surpass the cyber domain by affecting the physical world, meaning that cyber security remains an international priority. In this context, cyber security can be described as the combination of all activities and practices designed to protect a population's privacy, critical infrastructure and electronic components (National Academy of Sciences, 2015). Nevertheless, this definition of (cyber) security contrast with a classical designation of what security means for IR, focusing almost exclusively on state actors. To determine the role of cyber security within this field, it is necessary to return to the fundamental questions of security studies: *from what, for whom and by what means?* Literature so far, has shown that the main challenges derived from cyberspace correspond to the fast-paced development of new technologies coupled with the growth in number of cyber-centred activities and actors (Choucri and Clark, 2019). As result, cyber threats are shaped by the cyberspace design and deployment of these technologies for cyber conflicts, as well as the intents, motivations and capabilities of non-state actors. These issues would explain cyber security from what (Carr, 2016).

Furthermore, reports on cyber-attacks targets show that these attacks can occur arbitrarily in any layer of cyberspace to a varied spectrum of users (Shull & Hilt, 2021). Thus, *for whom* would policies on cyber security help to protect? In the present, regulations directed to the deterrence of harming cyber activities are divided into: damages suffered by computer technology and hardware components, and the attacks that have a more direct impact on users (Li & Liu, 2021). This would correspond to the physical and to some extent the platform layer, and the people's layer respectively. Moreover, research has found that sometimes the most targeted entities include businesses from the private sector that have greater control over the cyberspace (Hiller & Russell, 2013). Cyber-attacks launched against states have also increased in recent years, although goals are based on causing damage that would cross into the real world, or due to conflicts occurring in the real world (Nye, 2022). Conversely, the application of a holistic cyber security into the cyberspace, as well as other practices and strategies would cover the *by what means* question (Carr, 2016).

However, this is still covering a minimal part within the big picture that is the cyberspace, with the security question *from what and by whom* being largely underdeveloped. Until now, states have focused on cyber threats involving other states or non-state actors that might be affiliated with certain states as proxy organisations (Klimburg, 2011a). However, the proliferation of non-state actors acquring the necessary capabilities to launch attacks has made the question *from what* to become more significant. This is because it is difficult to determine whether individuals act alone or on behalf of a state, as participation in cyberspace allows to transcend bounds of territoriality and identity (Choucri and Clark, 2019). This has raised the attribution dilemma that render most cyber operations difficult to respond to as cyber-attacks cannot be, most of the time, fully tracked back to the perpetrators. On the other hand, within the cyberspace there seems to exist some influential cyber entities such as private actors that seek to expand control and establish their legitimacy (Carr, 2016). Thus, as states assert their control and dominance on cyberspace, the interactions with these other cyber actors might lead to a disruption of the internal perceived model of security equilibrium within the cyberspace. Showing how much uncertainty still exists regarding who controls who within the cyber domain as there seems to be a political struggle of governance.

# The Rise of Net States

## The "Old" Evolution into the "New": A Neorealism Framework

In contrast to the physical world in which international relations (IR) theories have been applied to historical and present events, the 21st century is cyber. Within this domain, as literature has shown, the political, social and cultural dimensions of modern societies are being profoundly transformed - creating new systems of meanings (Reveron, 2012). For nation states, this has resulted in the need to adapt governance practices better suited to the cyberspace, a paradigm shift not yet compatible with current theories. In traditional IR, the state is a central unitary concept of theories, policy and practices – a major anchor in the world of politics (Choucri & Clark, 2019). However, the contemporary international system composed of states, defined as sovereign (i.e., the highest legitimate authority that exercises control over a territory, free from intervention by external actors and independent) does not seem to have the same significance in cyberspace (Krasner, 2001; Philpott, 1995). In fact, the core structure and principles of cyberspace directly challenges this fundamental law. Besides, individuals and entities operating primarily in the cyber domain often develop virtual identities with the purpose of evading: detection, accountability and regulation (Branscomb, 1995). As consequence, the demands and pressure that states face to ensure the welfare of their citizens and protect national interests in cyberspace directly conflict with international politics.

By adopting a realist tradition, the dominant paradigm in international relations since the Cold War period, the incorporation of cyberspace into high-politics can be better understood. Realism in IR is based on a general set of assumptions that emphasise states as the most important actors, conceived as abstract units, interacting in an international system of anarchic nature (Perritt, 1998). Within this approach, a neorealism theoretical framework, further explores the international system as a structure: organised by its ordering principles, character of units and distribution of capabilities (Waltz, 2003). According to Waltz (1979), anarchy and not hierarchy is described as the ordering principle of the international-political system; where the absence of overarching authority compels a juxtaposition of units behaving similarly. This display of 'sameness' by states, additionally, it is shaped by both their functional differentiation and extent of their capabilities in assuring power and security. Nevertheless, in an anarchic international system, the presence of disorder and chaos does not remove the uncertainty associated with the expectation of interaction outcomes.

In international relations, generally states are well defined and all other actors are derivative of the state identity, while their actions are often observable and measurable in accordance to certain factors (Choucri & Clark, 2019). However, as informed by neorealism, uncertainty caused by states' pursuit of their own self-interests and self-preservation usually leads to a contested international system prone to power imbalances (Lobell, 2017). In a similar way when applied to cyberspace, competing actors whose intentions and motivations are not clear show outcome patterns relative to that of the international system. Although the level of uncertainty generated in cyberspace, by contrast, it is greater than that envisioned by neorealists. This is due to the added ambiguity feature of cyberspace - where the identity of other non-state actors is not well defined as it can easily be altered by mechanisms that support anonymity (Branscomb, 1995). Consequently, the emergence of other non-state actors exhibiting similar behaviours and levels of power as that of states in cyberspace supposes a conceptual threat to the neorealist framework. As states enter the cyber arena, they not only must protect their overall security, stability, safety and sustainability against cyber-attacks (Choucri & Clark, 2019). Now, they must also defend themselves against other influential non-state actors or entities that might undermine their sovereignty, thus, creating a security dilemma by increasing states' challenges.

While academic scholars have argued for a long time about the concept of sovereignty being in decline, this assumption is becoming more of a reality with the advent of the 4IR age (Grosby, 1997; Khan, 1992; Krasner, 2001;

Philpott, 1995; Spruyt, 2002; Wriston, 1997). Cyberspace, and specifically Internet, can pose a threat to sovereignty by challenging the main historical functions of the state which are: national security, regulation of economic activities and the promotion of moral values (Perritt, 1998). In terms of security, the ability of states to respond to many of today's cyber threats remains demanding due to cyberspace digital disruption and market dynamics (Singer, 2001). As states advance their national interests and migrate their critical infrastructure into the cyberspace, they become more exposed to the malicious activities of cyber-criminals, cyber terrorists, hackers and other non-state individuals or groups (Reveron, 2012). In addition, the proliferation of digital firms developing security solutions for individuals, businesses and governmental organisations has also diffused states' privileged position in providing national security. Therefore, in response to cyber security threats, states must collaborate with other non-state actors in cyberspace such as the private sector – creating complex cyber dependencies (Patel & Chudasama, 2021; Sigholm, 2013). On the other hand, private non-state actors such as social media platforms have undermined the economic and moral values functions of state. Through an algorithmic governance, these platforms revenue their activities by advertising methods – influencing people's information environment, and thus, their values and morals (Kreps, 2020). Hence, as the cyberspace continues to grow due to the evolution of technologies; the unitary significance of states seems to decline due to the fragmentation and relegation of security activities to other non-state actors.

Despite differences between traditional security problems and newer issues of cyberspace, states are attempting to reinsert their dominance in the cyber domain using digital sovereignty means (Cavelty, 2015b). In traditional international relations, as mentioned, the state (public) is the dominant authority, legitimised publicly by expressed social recognition. However, when any identified gap in either capacity or functionality is demonstrated by states, private authority tends to prevail (Hall & Biersteker, 2002). Furthermore, states restricted sovereign actions in cyberspace favours private authority salience for responding to many issues in the globalised world, characterised by a multi-stakeholder approach (Carr, 2016). This, in turn, is gradually blurring the line between public and private sector authority dominance. On one hand states are reinforcing the politisation of cyberspace while on the other non-state actors are exerting new forms of power influence, impacting neorealism conceptual unit being exclusively the state (De Gregorio & Radu, 2022). Thus, this 'old' theoretical framework exists as a basis upon which to build a 'new' cyber conceptual integrated framework.

## Cyber Sovereign Structures in Cyberspace: A Net State Model

> "What sorts of changes would alter the international political system so profoundly that old ways of thinking would no longer be relevant?"[1]

In the cyber-physical era, factors such as a globalised cyberspace, Internet hyper-connectivity and development of sophisticated technologies are generating new forms of authority. Every day, people engage in social or professional activities that are directly connected to the use of internet, whereas the number of companies that offer partial or complete digital services are rapidly expanding. As result, certain cyber entities are becoming powerful enough to pursue their own interests, whereas states' sovereignty is becoming increasingly contested (Rizvi, 2018). This raises questions regarding the inclusion of the anarchic cyberspace into the established structure of the international-political system, particularly in the definition and regulation of these cyber entities. Although, not officially recognised as legitimate counterparts or derivatives by most states, naming phenomena in cyberspace that mirrors the physical world is becoming a common practice. For instance, using terms such as virtual, online or that start with the prefix e- to signal presence in cyberspace, as in the case of governments taking initiatives to deliver efficient services via cyber venues in the form of 'e-governments' (Choucri & Clark, 2019). Therefore, how to define the character of units that echoes the influence and authority status of states in cyberspace? To name this novel phenomenon, this dissertation proposes 'Net

[1] Waltz, K. N. (2000, p. 5). Structural Realism after the Cold War. International Security, 25(1), 5–41.

states'.

Recently introduced by Wichowski (2017), the term 'Net state' is a reference to non-state actors or collective internet-based entities that operate largely in the cyberspace. These Net states are characterised by possessing sufficient political and socio-economic power and a globalised operational model with the objective of preserving their digital territory and integrity (Harvey & Moore, 2022; Koley, 2017). As techno-political entities, they are comparable to states in organisation structure and as diverse in behaviour as the many states in the international system. In addition, Net states can set their own set of rules, norms and government bodies, largely determined by their main functions or activities and free from outside interference (Rizvi, 2018). In terms of population, it is largely built from digital communities that share common interests, values or ideologies, comprised by like-minded netizens following the Net states belief-agendas. For example, a Net state superpower in cyberspace could be an entity such as Google or Facebook, large international companies that have an active digital population comparable to the population size of the biggest states across the world, such as China or India (Muggah, 2017). Besides, these kind of influential Net states use the internet to offer services and social connectivity that usually have added benefits such as the creation of online identities that can be used for other Net states. Therefore, as states expand their power to enforce political regulations and security operations, the multifaceted functions of Net states in cyberspace acquire greater significance (Monti & Wacks, 2021).

From a strategic and tactical point of view, the study of Net states can be instrumental not only in the digital realm but also in the physical realm. Net states legitimacy and intrinsic power come from the collection and processing of large amounts of data through the active participation of digital actors confined in communities. At the same time, this generates belief-driven agendas and a supply and demand business operational model upon which different multi-stake holders rely on (Rizvi, 2018). Therefore, depending on the type of net states and their physical or geopolitical ties to a particular nation state, if these ever get compromised there could be serious repercussions to national security and protection of citizens. On the other hand, Net states continuous evolution via incorporation of innovative technologies could incite new forms of governance leading to a new world order (Monti & Wacks, 2021).

Much of the current literature on Net states and their globalised impact within international relations has focused on the understanding of these cyber governing bodies. Some studies have examined the comparative nature between current yet decaying concepts of nation states in favour of emerging net states (Lancelot, 2020). Other studies such as Harvey, (2021) have focused on the development of a framework that combines theories from different disciplines; aiming for a deeper knowledge on collective internet entities and actors, and cyber statecraft to achieve strategic ends. As result, these literature trends have led academics to develop research that compare and analyse structural conceptual frameworks of Net states. A common example being that of identifying and labelling Big Tech or other dominant internet platforms as powerful Net states independent to traditional governments (Fukuyama, Richman, & Goel, 2021). Whereas other critical approaches such as Tiedke (2022) have argued in favour of using alternative terminologies to refer to this phenomenon. For instance, Tiedke (2022) proposed to use the analogy of 'self-statification' to compare national states to digital powerful platforms and their ability to govern themselves. Meanwhile, Harvey & Moore (2022) further deconstructed the nexus between national states and Net states to exemplify different control dynamics, like that of client Net states.

Nevertheless, Net state as a concept and exact definition remains subject to debate due to their relative new inclusion in academic literature as a phenomenon to study. In practice, Net states can be associated to many non-state groups as long as they have the enough influence and power to command authority and control in cyberspace. Examples associated to this include, but are not limited, to multinational digital corporations, hacktivist groups, non-governmental organisations (NGOs), cybercriminals and cyber terrorists (Reveron, 2012). However, there is still a relatively small body of literature research dedicated to the actual role of net states within the international security system. Thus, much uncertainty continues to exist regarding who controls who within the cyber domain as there seems to be a political struggle of governance.

## Identifying the Phenomenon of Net States in Cyberspace

Recognising relevant entities as Net states among the large pool of non-state groups requires a range of frameworks and strategies that address their unique characteristics and operations. Digitally empowered, Net states portray a flexible character regarding governance organisation in cyberspace – arguably necessary to operate effectively in such a dynamic and volatile environment. Therefore, in contrast to established nation states governed by centralised domestic institutions, influential cyber entities possess limited physical institutionalisation, if none (Choucri and Clark, 2019). Previous attempts at categorising non-state actors by evaluating factors such as size, internal structure, motivations, capabilities and operations have often resulted in a variety of typologies being proposed (Bussolati, 2015; Sigholm, 2013). This diverse classification generally covers private corporations, cybercriminal or terrorist networks, hacktivists, and even cyber militias, a wider scope than the plausible for analysis purposes. While the ensemble of non-state entities might be varied, this section focuses exclusively on the cases of Big Tech, the hacktivist collective Anonymous, and the media non-governmental website Wikileaks. Hence, these cyber entities' role, structure, operations and functions are analysed through their historical development and current role and position in the cyberspace. Focusing on the conceptualisation of Net States as a unit for further theoretical analysis, it will attempt to prove its effectiveness for strategical, and ultimately security purposes.

### Asserting dominance: The case of Big Tech during the Trump administration

Perhaps, the most notorious digital entities often equally associated to the 'real Net States' are the collective information technology companies —

known as Big Tech. Used as a reference for the predominantly US-based companies of Alphabet (Google), Amazon, Apple, Meta (Facebook), and Microsoft; this term started to gain traction around 2013 as result of the growing interest on the infrastructure of cyberspace and its governing authorities. Promoted by the digital era and a lack of regulations, the proliferation of digital firms that would act as intermediates in the cyberspace, did not suppose, at first, a direct challenge to traditional notions of governance and sovereignty. However, it was not until the sequential events that succeeded the election of Donald Trump as the 45th president of the US that the term Big Tech regained popularity in 2017. This time, as a pejorative term to reflect the potential of these digital entities to interfere inside and outside the cyberspace (Oremus, 2017). Thus, raising questions about how to define and regulate Big Tech impact on real-world politics (Sitaraman, 2020).

Having a long history of internet-related business activities since their establishment, Big Tech companies rode on the technological revolution of the digital era with their innovative services and products. Examples of this include: Google's development of its famous search engine, the founding of social media networks such as Facebook and Twitter, the smartphone model introduced by Apple and a digital marketplace by Amazon just to name a few. Nevertheless, the economic ventures of these companies to raise to their powerful global positions have not been free of controversies. Apart from criticisms related to the monopolisation of market shares in their respective economic avenues (Sitaraman, 2020). Big Tech gradual exhibition of attitudes similar to those of nation states were salient in contrast to other similar transnational corporations and industries (Oremus, 2017). Having to ensure a long-lived economic survival under a new normal context of disruption in cyberspace and following an increase of cyber threats, Big Tech undertook a series of organisational and practices changes. These ranged from self-regulation norms to the creation of private foreign policies, diplomacy negotiations and security apparatuses (Chachko, 2021).

The tensions between Big Tech and nation states, however, reached its peak following the scandal of Cambridge Analytica meddling into the 2016

US presidential elections. Marking 2018 as the year of critical juncture between the private and public sectors, and revealing the, until that moment, unperceived fact that these companies were exercising a significant control over the cyberspace (Chachko, 2021). During this case, Cambridge Analytica –a British political consulting firm– was exposed for harvesting millions of Facebook users' data, previously collected through an app called 'This Is Your Digital Life'. Initially developed and deployed for research purposes, the real objective of this app was to ask a series of questions that would be used to build a psychological profile of its users. Nevertheless, the app was able to compile personal data from the consenting users and their Facebook friends. Among the information included for the analysis were public profiles, page likes, birthdays, and in some instances even the location was recorded (Cadwalladr & Graham-Harrison, 2018). Afterwards, it was argued that this data was used by Cambridge Analytica to assist with the political campaigns of Ted Cruz and Donald Trump. By determining users' personality traits from their Facebook activity, it offered the dissemination of micro-targeted advertisements via different platforms. Then, ads were divided into supporters and swing voters, influencing voters' behaviours to increase the probability of winning the presidential elections (Smith, 2018). For Facebook, on the other hand, the consequences of this scandal demonstrated the platform's datafication practices. Although, this scandal was labelled as a 'major data breach' by media, being the original raw data still accessible by authorised entities. Facebook top executives, including Mark Zuckerberg, emphasised rather a 'breach of trust', seeking to minimise their dubious codes on privacy and management of users' data (Wong, 2018).

Nonetheless, the association of Cambridge Analatica with the 2016 presidential elections outcome supposed a stark dark contrast with Facebook previous efforts at reducing misinformation on its platforms. To contribute to the integrity of elections and civil participation, Facebook's cyber security, threat disruption and global elections teams were tasked in uncovering and disrupting information operations leveraged to manipulate public debate (Chachko, 2021, p. 75, 76). This involved the monitoring and analysis of users' accounts for proactive takedowns on the grounds of suspicious behaviour, which in 2017 even led to the disintegration of a network linked to the Russian Internet Research Agency (IRA) in their attempts to influence the 2016 US election (Chachko, 2021, p. 77). Therefore, this suggests that Facebook, despite showing a neutral stance and dedication to combat misinformation, might exert influence on their users through their business agenda pursuit. Moreover, a journalist investigation in 2021 exposed Facebook's awareness "in acute detail, that its platforms are riddled with flaws that cause harm, often in ways only the company fully understands" (The Wall Street Journal, 2021, p. 1). The investigation, that covered research reports, online employee discussions and drafts of presentations to senior management, reinforced the fact that previous scandals, and subsequent punishments on the tech giant did not affect its internal operations. On the contrary, these documents suggested that the identification of issues, such as ensuring the physical and psychological well-being of its users, were not being fairly addressed. Besides, attempts at solving issues pertaining security, such as the rampant spread of misinformation, hate and suppression of dangerous political movements on the platform, according to these documents still failed to deliver effective solutions. And yet, Facebook tactics to address them seem to resemble states engagement on geopolitical topics (The Wall Street Journal, 2021). Thus, evidencing that any internal conflict of interest would favour the company's benefit over the public good, even if it means rebelling against national regulations.

Following Big Tech 2018's series of events was Google's revisited goal to dominate the Chinese digital market amid a contentious US and China economic trade war. Considered the largest in the world, Google has continuously believed in the success of entering the Chinese digital market (Budnitsky & Jia, 2018; Yeo, 2016). Therefore, after a long withdrawal from the country, Google embarked on new negotiations with Chinese big technological companies such as Tencent to collaborate in future innovative digital projects (Chandel et al., 2019). However, in 2018, a journalistic report revealed that the company was actually working on the Project Dragonfly, a censored Chinese version of its search engine. The discovery caused heavy criticism and backlash from employees and human right activists' alike, with

US Vice President Mike Pence personally having to call the company to terminate Dragonfly (Sheehan, 2018). Thus, exposing Google's seemly treachery act against the US national interests and foreign policy at that moment. Because Google, as a representative US home-brewed technological company, carries the democratic values of its parent nation — emphasised in their own statements "about making technology work for democracy" (Walker, 2022, section 5). On the other hand, and in a similar way to Facebook, Google activities focused on the restriction of foreign entities from misusing their services has allowed a close collaboration with national stakeholders. An example of this being Google assembling of the Threat Analysis Group, which in 2019 disrupted Russia-affiliated influence operations that targeted several African nations. Their own think tank Jigsaw, with the mission to build technology that addresses security challenges threatening an open society, was also an initiative that does not seem to align, however, with their economic interests (Chachko, 2021). Hence, Big Tech stance on geopolitical issues and interactions with other nation states implies that their businesses agendas would prevail over their allegiance to their national countries.

Furthermore, the gradual Big Tech assertion into the cyber-international relations matters due to their significant control over the flow of global information took an unprecedented turn on 2021. In the aftermath of US presidential elections of 2020, the then President Donald Trump –an avid Twitter user– who had run most of his presidency communications and even policymaking from this social media platform was essentially labelled a national security threat (Chachko, 2021; Hennig, 2021). Originated from Trump baseless widespread dissemination about the 2020 elections being rigged, it culminated in the January 6th Capitol Riots after a mob of Trump supporters violently entered the premises. This incident resulted in Trump being 'permanently suspended' from Twitter (Twitter, 2021), along with the suspension of around 7,000 accounts associated with the conspiracy movement QAnon (Chachko, 2021, p. 83). Trump banning from other popular sites such as Facebook, also drove his supporters to transition into the 'free speech' defender social platform called Parler. Nonetheless, this was a short-lived action as the other Big Tech giants took serious measures such as Amazon cancelling its Amazon Web Services where the platform was hosted, while Google and Apple removed the app from their stores (Hobbs, 2021). Although, in essence the accusations made by Trump against social media platforms were about free speech, the argument posed by these platforms to justify their actions was Trump incitement to violence. The stance of Twitter in the historical ban of a head of state sparked debate about digital platforms moderation policies and self-regulation practices. As this posed provocative questions regarding the power in influencing and limiting content posted by even the accounts of powerful global leaders, and how common this practice would become in the future (Scapolo, 2021).

Therefore, these events involving Big Tech demonstrate that their gradual shift towards nation states traditional domains of security and geopolitics has become a double-edged sword analogy (Kreps, 2020). While there are many instances of these companies cooperating with US officials and government bodies in the protection of the country, their economic venues to capitalise on as much digital shares as possible shows the opposite. Instead, their business agendas seem to gain priority over US national concerns as pointed out by later congress hearings directed to break up the hegemony of Big Tech (Sitaraman, 2020). Additionally, the massive amount of data that these companies process and their ownership of critical cyberspace infrastructure means that Big Tech has dramatically evolved into sovereign digital states. Spreading ideologies and values at an international level, while influencing and controlling the behaviour of their users through targeted advertisements (Gu, 2023; Schmidt & Cohen, 2010).

## The case of Anonymous: Paving the way towards hacktivism

Lurking across the different layers of cyberspace, without physical territories bounding them except the common pursuit of political, social or religious causes are hacktivists. These often-decentralised collectives use the internet to coordinate activities, in this case ‘hacks’ to expose injustices, raise awareness and create public debates. Hacktivism has its roots in hacking which is related to the legal or illegal manipulation of computer systems or networks; however, what distinguishes hacktivists from hackers is their inherently political and frequently illegal conduct (Kelly, 2012). Targets can include powerful individuals or commercial institutions and state governments or institutions and does not necessarily align to democratic values. Therefore, hacktivism can be directed towards conventional political oppositions or support different political ideologies that counter jurisdictions of the attacks. In addition, hacktivism is typically anonymous and can enjoy significant power if a collective movement manages to reach sufficient people to support a cause. Thus, providing hacktivist collectives the ability to attack critical infrastructures, expose classified government information, and spread malware to a large number of commercial, official or even private computers (Sorell, 2015, p. 392).

The current embodiment of the ideal and powerful hacktivism collective with Net State-like characteristics is Anonymous – a household name responsible for 45% of cyber-attacks in recent years (Mayersen, 2019). Originated from the anime-dedicated Internet forum 4chan in 2003, Anonymous was perceived as a small group that coordinated actions in the form of “trolling” against other Internet communities. Targeting individuals or communities that had disagreeing ideas from them, these campaigns were merely performed as means of having fun (Volle, 2023). Subsequently, Anonymous inconsequential Internet pranks continued for a couple of years without visible impact outside cyberspace until the 2008 clash with the Church of Scientology, when the hacktivism word became a concrete reality. From this incident onwards, Anonymous developed into an international Internet collective that would engage in digital and physical actions. Formed by a network of individuals with similar interests and goals under a decentralised command structure operating on ideas rather than directives (Anonymous, n.d.; Kelly, 2012).

“We are anonymous

We are legion  
We do not forgive  
We do not forget  
Expect us."[2]

On January 2008, Anonymous posted a video message directed to the Church of Scientology promulgating their manifesto in defence for a free Internet space and a call-to-arms for people – formally launching Operation Chanology (AnonymousNetherlands, 2011). The operation was organised in response to the forced removal of a 'leaked' Tom Cruise YouTube video about the Church of Scientology. Calling it a censorship act, Anonymous swiftly set up a wiki for the project hosting Scientology documents that the Church considered proprietary and directing supporters to download denial of service (DoS) to attack Scientology websites (Singel, 2008). Other attacks included linking the term 'Church of Scientology' with 'dangerous cult', making prank calls and sending 'black faxes' which consisted on the receiving Church's fax machines production of endless black pages to waste ink (Anonymous, 2020; Volle, 2023). In addition, a press release declaring a 'War on Scientology' soon was followed by a massive coordination of physical worldwide protests outside Scientology centres, spread through several social media platforms (Volle, 2023). Other 'legal' form of protest involved getting the Internal Revenue Service to investigate the Church's tax-exempt status in the US. This would further prevent media portrayal of the Church of Scientology as a victim of religious hate crime, as the Church had declared themselves (Eordogh, 2014). What Anonymous ultimately desired was a completely removal of the Church from the Internet, driven by previous conflict of the Church of Scientology against the Internet, known as 'Scientology vs Internet' (Singel, 2008). Thus, approximately more than 6,000 Anons took part in the operation, while in-person protesters that wore Guy Fawkes masks to protect their anonymity converted this symbol into its trademark identification (Kelly, 2012).

[2] Anonymous. (n.d.). *About Anonymous*. Retrieved July 18, 2023, from Anonymous Hackers: https://www.anonymoushackers.net/anonymous-history/

Anonymous moral retribution success through Project Chanology marked a new era for more politically motivated global operations, fighting in the name of Internet freedom and lulz. Nevertheless, this type of digital and physical hacktivism would take an even greater turn on the year 2011 with Anonymous endorsing real-life protests with far larger repercussions. One of this was Operation Tunisia in relation to the Arab Spring in 2011, which was a series of anti-government protests, uprisings and armed rebellions that affected the countries of Tunisia, Libya, Egypt, Yemen, Syria and Bahrain (Al Jazeera, 2020). A large-scale revolution during the digital era, the Arab Spring was characterised by the use of social media platforms and power of information, which inspired Anonymous to intercede (Eordogh, 2014). Operation Tunisia involved the defacement of the government websites, publishing even a protest letter on the Prime Minister's homepage to stop the oppression of people and suppression of Internet. However, arrests of internet users persisted through tactics such as censoring websites and phishing of people's social media logins information – usernames and passwords. Therefore, to resist this, some Anons started to develop alternative communication systems sharing digital care packs – technologies collected to bypass privacy restrictions in Tunisia (Jordan, 2015). A customised message was included in the pack to encourage Tunisians who were putting "themselves at risk - by passing news and software back and forth between online Anons and protesters on the outside world". The text read as follows: "This is your revolution. It will neither be Twittered nor televised or [sic] IRC'ed. You must hit the streets or you will loose [sic] the fight. Always stay safe, once you got [sic] arrested you cannot do anything for yourself or your people. Your government is watching you" (Norton, 2012, p. 15). Gradually, Operation Tunisia kept unfolding by demonstrating similar efforts in the subsequent protests that followed suit during the Arab Spring of what became known as the Freedom Ops. Although, it remains difficult to analyse the extent by which these Anonymous operations caused the overthrow of state leaders, it assisted with the flow of information (Jordan, 2015). Being this, the most significant aspect that compelled Anonymous into upholding impactful social justice by empowering people to lead their own revolutions.

While Operation Tunisia was an early demonstration of Anonymous enacting foreign politics, operation Occupy Wall Street several months later would parallel domestic politics. “All of us have a reason to go to New York City on September 17th: to occupy Wall Street” read a statement published by Anonymous that month in 2011 (International Business Times, 2011, p. 3). The movement, endorsed by Anonymous, gained notoriety when activists encamped in Zuccotti Park near Wall Street were protesting against: corporate influence in American politics, racial economic inequalities and infringement of human rights. Within the cyberspace, however, Anonymous' simultaneously launched an online campaign –URGE– via Twitter turning a New York city-centric event into a national and later international protest. Bringing into the encampment site more protesters that “challenged local police agencies in ways not experienced since the 1970s” (Gillham, Edwards, & Noakes, 2013, p. 81). The coordinated action and rapid diffusion of information that Anonymous was directing through the social media platform maintained the protests peaceful. In a similar way to Operation Tunisia, on-site Anons would be the ones communicating back and forth with the other Anons online (Kazmi, 2011). Although, according to an internal memo by the Department of Homeland Security a warning was issued to financial companies to stay vigilant about a cyber security threat from Anonymous (Wyler, 2012). Their role during the Occupy Wall Street movement remained merely as a symbol of political endorsement; despite a controversial low-impact cyber-attack to the New York Stock Exchange website that was thought to be done by Anonymous (Eordogh, 2014). Thus, the Internet collective's actions during this operation showed their capacity to organise and mobilise in support of social causes rather than just disrupt and attack.

Anonymous trajectory as a global phenomenon after Operation Chanology in 2008 steadily allowed the coordination of more cyber operations that peaked between the years of 2011-2012. Just in one year, operations such as Operation Tunisia and Occupy Wall Street amongst others, provided Anonymous a positive reputation and international recognition “as digital freedom fighters and online Robin Hoods” (Eordogh, 2014). This further consolidated Anonymous key characteristics, being: “(1) an unrelenting moral stance on issues and rights, regardless of direct provocation; (2) a physical presence that accompanies online hacking activity; and (3) a distinctive brand” (Kelly, 2012, p. 1680). Additionally, the collective influence “lead major cybersecurity companies to characterise 2011 as the ‘year of the hacktivist’” (Karagiannopoulos, 2021, p. 6), while in 2012 the Time magazine declared Anonymous one of the “100 most influential people” in the world (Volle, 2023, p. 7). Therefore, this case demonstrates the power of collective entities such as Anonymous in attracting netizens and launching of highly organised operations that might undermine nation states cyber capabilities. For instance, Anonymous (n.d) stated that only in 2014 there were over 10,000 Anons divided into a subset of groups with about one thousand active hackers. Although, their self-proclamation as an international movement without a single identifiable leadership nor membership as anyone can potentially become an Anon remains contentious (Kelly, 2012). Whilst Anonymous had had internal dissent over their messages and operations, the collective has shown their capacity to unify disparate factions in several of their grand operations. This, in return, has opened the possibility of decentralised collectives becoming organised and focused groups reinventing the hacktivism game by developing hacktivism tactics for more targeted cyber-attacks.

## Ally or adversary?: The case of WikiLeaks

In the context of cyberspace, there are entities that exist predominantly within a particular layer yet have the potential to exert substantial impact on the global cyber-political landscape. Accordingly, this applies to (non-governmental, non-profit) organisations using the internet as a platform to garner significant influence and civil followers to carry out their missions (Schmidt & Cohen, 2010). Focused on humanitarian or social causes, the ability of these entities to operate without judicial restrictions or boundaries imposed by governments could provide an advantage in cyberspace. As organisations whose primary function is advocacy and the raising of fundings, the interactive nature of the Internet has enhanced the dissemination and advertising of their messages while acting as a fundraiser tool. In addition, the easiness by which these organisations can foster civic engagement on their websites through the creation of virtual communities can promote sociopolitical movements on the real world (Brainard & Brinkerhoff, 2004). However, in a disruptive environment such as the cyberspace, building public confidence through the utilisation of information might actually have adverse consequences.

This is exemplified by the landmark case of WikiLeaks –a multi-national media organisation and associated library– founded by Julian Assange in 2006 (WikiLeaks, 2015, p. 1). Self-described as a non-profit organisation, it specialises in the analysis and publication of sensitive information with the mission of promoting transparency and accountability. Among the large datasets of stored information and the more than 10 million documents are: classified or censored documents and otherwise restricted official materials of political, diplomatic or ethical significance (Hindman & Thomas, 2014). Furthermore, to protect itself and their anonymous sources (whistleblowers), WikiLeaks legal framework consists in the use of web servers distributed across several jurisdictions (Symington, 2009). Additionally, it maintains contractual relationships and secure communications with several other major media organisations across the world (WikiLeaks, 2015, p. 4). However, despite this privileged position in the cyberspace, this 'transparency' online platform has posed numerous times as a challenge to states' leadership, with conflict ramifications of international matter. Hence, becoming a noteworthy non-state entity on the political sphere, managing to capture the attention of netizens through polemic disclosures and leaks (Lovink & Riemens, 2013).

> "WikiLeaks is a giant library of the world's most persecuted documents. We give asylum to these documents, we analyze them, we promote them and we obtain more." [3]

[3] WikiLeaks. (2015, November 3). *What is WikiLeaks*. Retrieved July 19, 2023, from WikiLeaks: https://wikileaks.org/What-is-WikiLeaks.html

WikiLeaks accrual disputed reputation began since its initial years with the sporadic release of materials that embodied the character quality of their subsequent disclosures. For instance, in 2007, Julian Assange acquired a collection of millions of documents through the data mining of The Onion Router (Tor). Although, not verified, the story narrated from these documents was about a Somali rebel leader who encouraged assassins to execute government officials. Next, the website released a US Army manual of standard operating procedures for the military overseeing of terrorism at the detention facility in Guantánamo Bay, Cuba. In 2008, WikiLeaks posted leaked emails from vice presidential contender Sarah Palin, and faced legal pressures from the US which led to the creation of mirroring URLs in other countries. The publication of some Scientology documents also brought legal charges against the website by the Church to which WikiLeaks responded by releasing even more documents (Ray, 2023). However, the most high-profile leaks in history of classified information occurred between the years of 2010 and 2011, provided to WikiLeaks by Chelsea Manning (a.k.a Bradley Manning) a former US intelligence analyst.

The first release in April, titled ‘Collateral Murder’, was a US military video that showed how a helicopter launched airstrikes killing intended targets and civilians in Baghdad, Iraq. Just on YouTube, the video accumulated more than ten million views – considered the breakthrough moment for WikiLeaks. However, some months later, WikiLeaks would publish yet the largest-scale releases from the Middle East wars, namely the Afghan War Diaries and later the Iraq War Logs. The Afghan diaries included the release of 77,000 cables, while the Iraq logs were composed of 391,832 documents published at once that covered the period from January 1st, 2004, to December 31st, 2009. By the end of the year, WikiLeaks ended up releasing US diplomatic cables under the project name Cablegate. These cables contained confidential and often candid communications between U.S. diplomats and foreign governments, providing insights into international relations and diplomatic activities. Just on the first day 220 cables were released, followed by a gradual publication of a total of 251,287 cables of which 40% were classified as confidential and 6% as secret (15,652 cables) (Maurer, 2011, p. 11, 12). Cablegate files distribution, however, was provided by major media outlets across the world such as the New York Times, the Guardian, Der Spiegel, Le Monde, El País, and later to other media organisations. This caused some of the material to be withheld after careful selection and redaction made by these media organisations, while about two-thirds of news reports falsely commented that all had been released (Benkler, 2011).

The consequences that ensued had a wider and systemic impact for the United States – at the state and international levels. In regards of the information about the Afghan and Iraqi wars, it revealed shocking details that led watchdogs to revise their estimations for civilians' casualties. After the leaked information, the total number of deaths amounted to over 10 thousand committed by the American Armed Forces. For the public, this meant that the US covered the truth about the real impact of the wars and the aforementioned humanitarian disaster, being worse than initially stated by official sources (HISTORY, 2019). Abroad, Taliban forces claimed to analyse the published sensitive information for tactical purposes, being the most critical the diplomatic cables which uncovered worldwide infrastructures for the US. Moreover, these cables created a fear of possible diplomatic mistrust between the US and governments around the world. Therefore, many officials within the US and abroad had to leave or be relocated because of the published information on diplomatic assessments, confidential conversations and intelligence gathering activities. Although, previous assessments of harm by government officials and media representatives pointed out that WikiLeaks releases were 'embarrassing but not damaging' (Maurer, 2011, p. 26). This, nevertheless, resulted in the then president Obama having to speak with a number of head of states, whereas Vice President Joe Biden branded WikiLeaks' founder Julian Assange a 'high-tech terrorist' (Hindman & Thomas, 2014, p. 542).

The rhetorical framing of WikiLeaks as a global threat, in turn, allowed certain actions to be pursued by the US that would not have been possible otherwise (Benkler, 2011). On the legal aspect, the Department of State and the Department of Defence conducted a formal criminal investigation that led to the arrest of Chelsea Manning. Besides, a federal court secretly asked Twitter to give information related to the WikiLeaks account to help locate Julian Assange, a similar procedure used with Google to pry on WikiLeaks staff's email data (Sifry, 2011). On the technical aspect, American hackers targeted WikiLeaks website by launching DoS cyber-attacks, and the speculated attempt of US government to pressure the domestic provider of Domain Name System (DNS) into disabling wikileaks.com. The US government also pressured Amazon to stop hosting WikiLeaks website on its servers (Choucri & Clark, 2019). Other activities in cyberspace involved private corporations such as Paypal, MasterCard and Visa halting donations processes to WikiLeaks. This resulted in the intervention of Anonymous by bringing the websites of these companies down in support of information openness (Maurer, 2011).

In essence, the international revolt caused by WikiLeaks sparked intense debates about government transparency, freedom of press and the balance between national security and public interest. On one hand, WikiLeaks supporters emphasise its critical online role in cyberspace of journalistic value for exposing corruption and government wrongdoings (Hindman & Thomas, 2014). For national states, on the other hand, WikiLeaks represents a challenging dilemma. Particularly for the US as a superpower, defender of democratic values and proponent of a free and open Internet space (Pieterse, 2012). Thus, irrelevantly of Julian Assange ongoing legal procedures as the founder and central player in the release of the documents, no other non-profit cyber entity has managed what WikiLeaks did (Lovink & Riemens, 2013). Hence, WikiLeaks structural organisation and sustainable presence in cyberspace as a defender of free information (whether ethically correct or not) suggests the probable pilot phase in an evolution towards other non-state actors following suit.

## Net states as a unit of level analysis

The cases examined in this section were chosen as representations of the novel phenomenon defined as Net states. Overall, through the series of events illustrated above, these cases demonstrated traits and attitudes comparable with states as abstract units that have the potential to transform the current international world of politics. Firstly, in the case of Big Tech, these technological firms show a vast economic and political power, expressing a digital sovereign empire. Within their platforms (or digital territories), no other state actors can interfere, remaining independent and governed by their own norms. Secondly, in regard to collective groups such as Anonymous, their power resides on their ability to mobilise a large number of netizens and civilians for socio-political causes. As hacktivists displaying an offensive position, the impact of their operations had large-scale consequences. The peculiarity of Anonymous, however, is their trajectory from a trolling group to being the most recognised hacktivists culturally. In addition, despite their claim of being decentralised, some of their operations demonstrated a highly organised group, a model of operation that could be imitated by other malicious hacker groups. Thirdly, the unprecedented case of WikiLeaks highlighted the capacity of non-for-profit organisations having substantial impact on the security of a nation. This case also posed a division between those defending an open Internet space away from the intervention of states. Thus, the support received from within the cyberspace allowed the continued operations of WikiLeaks, irrelevantly of Julian Assange's exceptional situation. Hence, Net-States should be viewed as a matter relevant to the realm of high-level international politics due to their role in the management and control of cyberspace. This authoritative position allows Net states to be key decision-makers in matters relevant to cyberspace. On the other hand, Net states may disrupt the international security at any time to leverage their power and demonstrate their influence and power.

In the following chapter, the concept of Net states is going to be addressed within an international level approach to address theoretical implications under a security context. To further evaluate its value as a unit level that parallels the behaviour of national states in terms of power dynamics and disruption in the cyberspace.

# Cyber Power Dynamics and the Disruption of International Security

## A Global Internet Governance: Conquering the Cyber Realm

"On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather"[4]

Since its inception, the cyberspace, and specifically, the Internet's technical infrastructure that forms the global backbone of today's cyber world have been considered a neutral foundation (De Gregorio & Radu, 2022). However, the intervention of nation states to utilise this domain for political and security purposes has gradually disassociated from Barlow's (1996) declaration for an independent cyberspace. The rise of information and territoriality issues, in addition, has moved into the top priorities of states' agendas, questioning the power ramifications for the international system (Bronk, 2012). Therefore, as cyber politics become a reality by reshaping the international order, states' associated regimes are transforming the ways in which the Internet ought to be governed. Guided by the development of a common grounds system of laws, rules, policies, standards and practices, Internet governance has been proposed to serve as a multistakeholder structure (Shen, 2016).

Nevertheless, one of the main constraints of an Internet governance composed of state and non-state actors is the communication of interests to inform policy-making decisions. For states, this is just an opportunity to reinforce their digital authority and values through the leverage of diplomatic instruments to control the Internet (Kreps, 2020). For other non-state actors, it is about the creation of norms and standards through the leverage of technological innovation that compels states into forming alliances with them to demonstrate their legitimacy (Ibáñez Múñoz, 2021; Schmidt & Cohen, 2010). As result, not only sovereignty is being contested in the cyberspace, but

[4] Barlow, J. P. (1996). A declaration of the independence of cyberspace. Retrieved from Electronic Frontier Foundation: https://www.eff.org/cyberspace-independence

discussions about Internet governance are further fragmenting and polarising interactions among states and non-state actors alike.

To complicate matters, the division of cyberspace into different 'Internet ecosystems' is turning into a real possibility because of some states' initiative to apply sovereign rules to the lower layers of the Internet (Lambach, 2020). From a historical perspective, the Internet derived from US projects and technological developments, meaning that most components of the current physical architecture retain a illusory US influence (Ibáñez Múñoz, 2021; Knake, 2010; O'Hara & Hall, 2018). Nonetheless, the social and ideological values embedded in the architecture of cyberspace favoured freedom beyond national states' geopolitical constraints. Therefore, in the early development of cyberspace, states did not have rights to interfere in the virtual communities nor digital platforms that were forming in the Internet (Bussell, 2013; Schmidt & Cohen, 2010). Despite this, in the last decade, authoritarian regimes such as China, Russia and Iran have taken an advantage of cyberspace to promote national interests and reinforce their political control. A classic example being China, setting as an objective within their cyber security strategy to protect its cyber sovereignty, which additionally is sheltered by the Great Firewall – China's own technical censorship infrastructure (Chandel et al., 2019). Moreover, these states' advancement in technological capabilities are redesigning the values in the Internet, as well as expressing their aspirations to separate themselves from the global net. In the case of China, it is seeking to replace the IP backbone of the Internet with its own version named "IP Networking for Network 2030" (De Gregorio & Radu, 2022, p.70). Hence, present trends arising from the extension of states' ideologies into the cyberspace seem to affect the distribution of power and exercise of rights and freedoms.

This nexus between a state's political ideology and digital power has substantially rearranged the conventional power balance structure in the international system. In response to authoritarian states' cyber capabilities, even the laissez-faire democratic states have changed their stance towards Internet governance and digital sovereignty to implement control and regulations (Knake, 2010). For instance, although, authoritarian states generally employ surveillance and filtration tactics of cyber control, an increasing number of democratic states are also employing these tactics (De Gregorio & Radu, 2022). Furthermore, there are other conditions that are causing a diffusion of digital power in accordance to a domestic, regional or global scope. By way of illustration, Shen (2016) summarised these as: the geographical distribution of Internet users, the gap in data-related facilities and the possession of critical cyberspace infrastructure. In the first case, Internet users from weaker or developing states tend to form the majority of user population in the people's layer in contrast to developed states. Apart from having a large user-base, developed states are the ones that generate most of the influential digital firms targeting Internet users, and consequently, dominate digital markets. Additionally, these powerful states have a larger ownership over data-related servers and cyberspace infrastructure. Therefore, weaker states do in large part depend on powerful states to connect into the Internet and access the cyberspace. This creates huge disparities in power distribution among nation states, reducing the scope of governance largely to a domestic level (i.e., China, US) and regional level (i.e., Western nation states, the global South) (Ibáñez Múñoz, 2021). Thus, the exacerbated asymmetry in capabilities among states are affecting states' behaviours towards cyber security whilst altering polarity in the anarchic cyber international system.

These structural changes can be further exemplified by the little uniformity in cyber security strategies and operation policies of states across the world. Several literature reviews and comparative analyses have been conducted with similar findings. These are summarised by the desired goal of reaching international harmonisation and a common set of national actions, and its subsequent failure due to variations in the preventive, defensive and offensive measures and approaches described. For example, Luiijf et al. (2013) analysed a small cluster of 10 nation states' cyber strategies. Among the results, they emphasised the lack of standardisation in definitions of cyber security and criticised states' attitudes toward cyberspace threats not being sufficiently holistic. Likewise, they argued that in general these strategies were separate from their main national strategies and states did not take into consideration the risks of losing the population's trust over cyber incidents. In another study, Shafqat & Masood (2016) examined a larger pool of cyber security strategies (50), finding that almost all of the documents mentioned the establishment of incident prevention and response capabilities at national level. These were related mainly with the raise of cyber awareness of the population and better promotion of private-public relations. Nevertheless, the objectives and awareness campaigns indicated variations, with some even showing opposing actions to that stated on the strategies. Only the US, UK and Germany were the strongest in development of defensive objectives and enforcement of offensive tactics in defence of their cyber assets and capabilities.

At the regional level, however, the strategic value of these policy documents did not vary too much from the ones at a national level. When comparing NATO and EU cyber security strategies, Štitilis, Pakutinskas, & Malinauskaitė (2017) noted differences in scope and aspects considered by these strategies. The biggest difference, especially in the NATO case, was the lack of action and coordination in implementing studies into practice. Similarities, in contrast, were formulated around cyber resilience assurance, cyber incidents and cyber fights processes. As result, all these studies suggest that differences interfere in the achievement of unified and collaborative responses to cyber threats. Reinforcing power struggles when it comes to forming partnerships with the private sector – objective that is commonly described but mostly undermined. Thus, these discrepancies point towards a greater perception that tensions between states might be escalating in cyberspace, questioning the ability of states to maintain sovereign control (Faesen, et al., 2020, p. 1).

## Cyber Power and Conflict Escalation

The pervasiveness of anarchy in the international system enables different parameters for potential power shifts to occur among states. Historically, this transition of power from one dominant state to another was of common occurrence, however, power diffusion in cyberspace is a novelty concept of modern times. Power, like sovereignty, is a contested concept, difficult to measure if not clearly defined upon a contextual background. In world politics, power represents “the ability to affect other people to get the outcomes one wants”. Upon a cyberspace context, therefore, cyber power can be defined as “the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power” (Nye, 2010, p. 2-4). Nevertheless, interactions in cyberspace have diffused power among the different range of actors that are attempting to control and govern it. Factors like those mentioned above, as well as more prevalent issues such as anonymity and easy access are becoming variables outside the traditional power control of states (Klimburg, 2011a). Therefore, not only weaker states are able to exercise cyber power (hard or soft) by accessing to a range of cheap cyber capabilities. But, in addition, other non-state actors (e.g., private sector and individuals) can have access to such power as well.

Under neorealism assumptions, this power diffusion can be perceived as temporary due to state regaining control and returning the international system back into an equilibrium (Waltz, 2000). Within this power dynamic illustration, positive characteristics displayed by states that show like-minded attitudes learn or imitate others by implementing policies and security accordingly. Negative characteristics are confronted with higher competition among states as perception of malicious intentions and threats impact decisions that state take – related the logical security dilemma (De Gregorio & Radu, 2022). These assumptions would project scenarios in which states with greater cyber power are more likely to pursue their interests aggressively in cyberspace, while weaker states become defensive and reactive. States with similar motivations and ideologies would also form alliances or collaborate to achieve greater security in the international landscape.

A key determinant to transform the international system is the behavioural intersections between state and non-state entities such as the proposed Net states. As cyber power derives from the total sum of resources or capabilities a state can leverage to support itself, it is difficult to extract Net states from the equation (Klimburg, 2011a). The cyberspace is an ecosystem where these non-state entities retain most of the control and operations, hence, the security dilemma would apply in this situation as well. For instance, the euphemism used within the private sector, “attacking back”, refers to these private actors taking the issue by their own hands. In fact, opinions from surveys actually show that these companies tend to attack back (Deibert, 2013, p. 6). This indicates that cyberspace actors such as Net states posses the necessary resources to form part of the security dilemma in the international landscape. Similarly, this would mean that they can leverage their power for offensive operations, as in the case of malicious Net states, or as a defence to protect themselves.

Conversely, a dependency on Net states or other non-state actors to control cyberspace would add another layer of complexity to the neorealism power balance framework. Klimburg (2011a) argues that non-state actors (malicious) can be used by states as proxy organisations, either covertly or overtly, to execute cyber operations. For example, China and Russia have been accused of launching cyber-attacks against other nations via proxy hackers, although proven evidence is difficult to obtain due to the attribution issue. Meanwhile, the West realisation of this opportunity has been rather slow. Additionally, instances where there was a public and private collaboration were voluntary in nature, and it has involved mainly issues pertaining misinformation (Chachko, 2021). On the other hand, authoritarian states have leveraged the power of their private sector to maintain tight control in their Internet spaces. This further suggests that Western states must implement a whole-of-nation approach into cyber strategy policies and into action (Klimburg, 2011a). To ensure the protection of their national interests at an international level and not only domestic. Thus, increasing interactions in spheres of influence poses new questions regarding cyber system threatening behaviour creating potential for new types of contentions and conflict (Choucri & Clark, 2019).

Although the cyber security goal should be the preservation of cyberspace and a nation’s interests, cyber conflict based on power dynamics seems a plausible scenario in the not-so-distant future. Tracing back to the origins of Internet, it was not designed to be secure, rather it was intended for the ease of use by expecting users’ good intentions. However, this (in)significant detail has generated a cyberspace with offensive advantage over defensive operations (Nye, 2010). In addition, the sentiment towards cyberspace has gone from hope and freedom expectations to that of cyber phobia. As argued by Deibert (2013), observable trends in cyberspace are leading to contention mainly due to: alterations in communication systems, growing private sector control over data and sovereignty assertion. Likewise, other situations of conflictive nature such as cyberespionage, cybercrime and cyber terrorism are incrementing security fear and justification for strategy advancement (Klimburg, 2011a). Therefore, given the importance of securing information and technology, states might take advantage over their adversaries by using tools and techniques to respond to cyber-attacks (Lin, 2012).

In this regard, some scholars argue that the cyberspace is becoming a ground for greater conflicts in the form of cyber war through the signalling of a cyber-arms race (Junio, 2013). The constellation of cyber threats and uncertainty regarding the effective actions to take follow a neorealist narrative of competition as an outcome (Deibert, 2013). For example, Craig & Valeriano (2016) to support this argument, evaluated the cases of US-Iran and North-South Korea. Findings from the US-Iran case, presented the existence of cyber arms-race being driven by mutual insecurity. The Stuxnet incident caused a friction that led Iran to build up its cyber capabilities, which by contrast, was perceived as threat by the US. In the North-South Korea case, the cyber-arms race is rather the result of North Korea aggressive behaviour, leaving the South with the only option as to defend itself. Moreover, another important factor in an increased perception of cyber conflict is market dynamics. As the hub of cyber security digital firms and Dark Web markets are increasingly offering cyber capabilities either for offence or defence purposes, different states could have access to the same resources (Deibert, 2013). This, in return, would alter the current power equilibrium incrementing the polarity of powerful states. To this end, Healey (2011) envisioned a variety of hypothetical scenarios about how future conflict could look like, highlighting two plausible scenarios that comprises current status quo or the very-likely conflict domain dominated by large-scale cyber-attacks. The other two scenarios are based on radical ends of the conflict spectrum, where complete cyber security exists or complete chaos reign cyberspace.

Nevertheless, the current situation in cyberspace –that of status quo in Healey's (2011) scenario– overlooks other significant element in the prevention of cyber conflict escalation. Adapted from the neorealist framework, cyber deterrence refers to the use of cyber mechanisms to deter adversaries from engaging in activities that are perceived as threatening or aggressive (Rivera, 2015). This is a strategy often used by states to maintain their security in the hostile international system of constant competition (Waltz, 2000). From a legal aspect, measures such as the application of international law and norms of responsible state behaviour are applied as means of stabilisation, as in the case of EU Internet regulation initiatives (Faesen, Torossian, Mayhew, & Zensus, 2020). However, this remains insufficient as conflict in cyberspace can occur due to misunderstandings in communication ranging from tension escalation to full-scale conflict with greater security consequences.

Pressure faced by states regarding decision-making, for instance, can drive to the implementation of extreme solutions. An example being automated cyber-attacks in response to other states actions. However, as Caton (2013) noted, these solutions serve to escalate tensions into conflicts – recommending the better formulation of cyber strategies that rather focus on building resilience. The author also added that these types of defence tactics should be used in a gradual basis as means of signalling actions to other states. Additionally, Steiger, Harnisch, Zettl, & Lohmann (2018) performed an analysis of conflicts based on interactions between states and non-states actors recommending a level-headed approach to the interpretation of cyber conflicts. As among their findings they discovered that cyber conflict can actually be a product of politicisation of cyberspace rather than the result of a security dilemma. Thus, there seems to be potential for tension as states use the cyberspace to achieve strategic ends while others actively seek to stabilise political interaction (Cavelty, 2015b).

## Conflict and Redistribution of Power in Cyberspace:

## Interactions and Implications

Increasing global contention in spheres of influence between Net states and nation states can cause different types of cyber conflicts and disruptions in international security. In accordance with the arguments discussed in the previous section, the build-up of cyber capabilities, as well as cyber actors and entities' tendency to expand their activities would expose new points of friction. Therefore, while nation states continue to strive for control and power by imposing their own rules and ideologies, Net states, to protect their integrity, might decide to counteract such actions. In order to examine power dynamics and interactions, this section will attempt to prove the following hypothesis:

H: Net states retention of cyber power will challenge nation states' behaviours in cyberspace, hence, increasing the likelihood of conflicts impacting the real and cyber realms.

A similar method and coding procedure as that used by Gamero-Garrido (2014) will be applied to four recent cases covering a variety of Net state, non-state and state actors.

### Case 1: 'Guacamaya' hacktivists massive theft and leak of sensitive information obtained from Latin American countries — 2016-2022

***Actors Involved***

- Guacamaya - environmental hacktivist group advocating for 'Abya Yala' (Earth Alive)
- Mexican head of state Andres Manuel Lopez Obrador (AMLO) and Secretariat of National Defence (SEDENA)
- Joint Chiefs of Staff of the Armed Forces of Chile
- Private sector - mining and oil: Chile, Brazil, Colombia, Venezuela, Guatemala, Ecuador
- Private sector - technology: Microsoft, Zimbra

- General Attorney of The Nation of Colombia
- Ministry of Environment and Natural Resources of Guatemala
- National Civil Police and the Armed Forces of Salvador
- Joint Command of the Armed Forces of Peru

### *Actions*

The group Guacamaya infiltrated and hacked the computer systems of the security agencies of the Mexican government to extract sensitive confidential documents associated with the country's internal affairs. Among these documents, there were some health records of the Mexican president Andrés Manuel López Obrador (AMLO). They also gained access into the email servers of Mexican Secretariat of National Defence – SEDENA via Zimbra, a collaborative software suite, obtaining a total of over one million of documents.[5]

Guacamaya then infiltrated into the Armed Forces' servers of several Latin America countries including Chile, Peru, Colombia and El Salvador through a security breach found in Microsoft's Exchange application. After gaining access to the servers, Guacamaya leaked a massive number of emails and classified documents described as 'Top Secret' from the affected countries.

The office of the General Attorney of The Nation of Colombia also experienced a similar cyber-attack which targeted official emails from the staff.

Private mining and oil companies' computer systems were exploited by extracting emails related to the communications between civil servants and direct contractors.[6]

### *Affected Layers of the Internet*

[5] Diaz, R. (2022, September 30). Guacamaya Hackers: ¿Cómo lograron hackear a la Sedena? Esta es la increíble respuesta. Retrieved from Sdpnoticia: https://www.sdpnoticias.com/mexico/guacamaya-hackers-como-lograron-hackear-a-la-sedena-esta-es-la-increible-respuesta/

[6] Espinosa Robledo, N. (2023, January 8). Grupo Guacamaya hackeó la Agencia Nacional de Hidrocarburos y empresas del sector petrolero. Retrieved from El Colombiano: https://www.elcolombiano.com/colombia/hackeo-a-agencia-nacional-de-hidrocarburos-de-colombia-BH19780540

All layers: physical, platform, information and people.

### *Power Relationships*

Guacamaya as a hacktivist group committed the aforementioned cyber-attacks to express their political message in regard to environment policies. Their principal purpose is to live in harmony in the 'Abya Yala', an old indigenous term used to denominate the Latin American territory.[7]

Microsoft warned users to apply an important security update to avoid a vulnerability found in the application that would allow external interference. Nevertheless, none of the armed forces from the affected countries were aware of this warning.[8]

In the case of Mexico, there was an additional element which showed SEDENA's oversight in their report. The security exploit was opened for at least 11 months. In his regular press conference, the Mexican president AMLO confirmed the cyber-attacks, and added that all the information related to his health was 'true' in a claim for transparency.[9]

Colombia through a statement confirmed that its contractor *Telecomunicaciones S.A.* activated the necessary protocols of verification and mitigation to avoid further risks. In addition, the judicial system conducted an administrative operation of due process to inquiry the accountability and responsibility of the private contractor due to the cyber-attack to the Prosecutor Office.[10]

The Chilean government of Gabriel Boric, demanded for an executive summary of the cyber-attack and provided evidence to the military justice to determine accountability charges. According to the defence minister, Maya Fernández, the investigations should clarify whether officials from the Ministry of Defence were aware of these penetrations into their information

[7] Guacamaya. (n.d.). No somos defensores de la vida, somos vida! Retrieved from https://enlacehacktivista.org/comunicado_guacamaya4.txt

[8] See Diaz, (2022, September 30).

[9] BBC. (2022, September 30). Qué se sabe de Guacamaya, el cibergrupo clandestino que reveló los problemas de salud de AMLO y ha robado secretos a varios de países de América Latina. Retrieved from BBC: https://www.bbc.com/mundo/noticias-america-latina-63098421

[10] See Espinosa Robledo (2023, January 8).

systems.[11]

### *Outcome*

Latin American states later applied the required security patches to all the exploited servers.

Colombia was one of the most affected states by the hacktivist penetrations and subsequent leak of classified documents related to prosecutors, police and witnesses under protection.[12]

Until now, the number of documents published was only a small proportion from the total obtained. Therefore, these cyber-attacks could be considered as one of the worst for the Latin America region. The scale of security vulnerability is arguably the largest at a global level.

Despite the seriousness of the security breaches for the private sector, the affected companies did not receive any sort of compensation nor support to implement better policies of cyber security.

Guacamaya keeps demanding the cease of operations for the mining and oil companies to stop the exploitation and contamination of the environment in return of financial gains. They do also condemn the colonisation of 'Abya Yala', first by the Spanish empire, and now by the US; and the manifestation against capitalism because of the adverse consequences for the environment and societies. They claimed the cyber-attacks were a means of reparation to the damage caused to the environment to honour 'Pachamama' (our Mother Earth) and their ancestors.[13]

## Case 2: TikTok - an entertainment app or a national threat to the US? — 2020-present

### *Actors Involved*

[11] Sepulveda, N. (2022, September 22). Hackeo masivo al Estado Mayor Conjunto expuso miles de documentos de áreas sensibles de la defensa. Retrieved from Ciperchile: https://www.ciperchile.cl/2022/09/22/hackeo-masivo-al-estado-mayor-conjunto-expuso-miles-de-documentos-de-areas-sensibles-de-la-defensa/

[12] See Espinosa Robledo (2023, January 8).

[13] See Guacamaya. (n.d.).

- President Donald Trump from the United States of America (and later Joe Biden)
- Federal Bureau of Investigation (FBI), United States House of Representatives and United States Senate and Department of Commerce
- • Federal Communications Commission
- Private sector - technology: TikTok (ByteDance), Oracle Corporation
- Private sector- retail: Walmart
- Media sector: Forbes

### *Actions*

During the administration of Donald Trump, the White House threatened TikTok, a popular Chinese app (also known as DouYin), to ban it under claims of national security risks. According to the president, TikTok and its parent company ByteDance collected personal data from US users that the Chinese Communist Party (CCP) could have access to. Donald Trump, then, signed two executive orders targeting TikTok and WeChat, the two most popular Chinese apps. The executive orders commanded the Chinese companies to sell a majority portion to any American company, and that US businesses had to stop working with these Chinese apps within 45 days.[14]

At the time, Microsoft, the American Big Tech, was in negotiations to reach a deal on the possibility to buy TikTok ahead of the deadline set by President Trump, as well as services in Canada, Australia and New Zealand.[15]

The deadline was extended up to two occasions.

### *Affected Layers of the Internet*

People, information and platform layers.

[14] BBC. (2020, August 7). TikTok: President Trump signs orders to ban it in the US within 45 days. Retrieved from BBC: https://www.bbc.co.uk/newsround/53620689

[15] Yang, Y., & Goh, B. (2020, August 5). Timeline: TikTok's journey from global sensation to Trump target. Retrieved from Reuters: https://www.reuters.com/article/us-usa-tiktok-timeline-idUSKCN2510IU

### *Power Relationships*

The Department of Commerce banned TikTok downloads, making the app temporarily disappear from Apple's App Store and Google's Play Store.

As response, TikTok announced that it was going to take legal action by filling a suit against President Trump appealing to the First Amendment of the US Constitution. TikTok claimed that they were willing to pursue a full sale to an American company, therefore, the executive order was undermining a global business operation. The statement also appealed to the concept of free expression and open markets affecting foreign companies trust on US.[16]

Two federal courts approved a temporary junction that halted Trump imposed ban on the application, in case of not selling the company under the time frame given.

TikTok negotiations continued by talking with other US companies such as Oracle and Walmart, receiving approval by the White House.

Claims of espionage against TikTok were later confirmed in a special report published by Forbes. The report stated that based on internal communications, they found out that TikTok actually fired four high-level employees (two in US and another two in China). The reasons were related to cyber espionage against US journalists that were investigating the company. The ex-employees "gained access to IP addresses and user data in attempt to identify" possible interactions with ByteDance employees.[17] The journalistic publication reinforced the probability of Chinese apps such as TikTok posing a high-risk to the US national security and integrity.

TikTok confirmation of cyber espionage signs occurred in the middle of a tense situation for the company as it was being investigated by the FBI. Its chief told in a committee hearing about threats to US security that the Chinese government could utilise the application to "control software on millions of devices and drive narratives to divide Americans over Taiwan or other issues."

[16] BBC. (2020, August 7). TikTok threatens legal action against Trump US ban. Retrieved from BBC: https://www.bbc.co.uk/news/business-53660860

[17] Baker-White, E. (2022, December 22). TikTok Spied On Forbes Journalists. Retrieved from Forbes: https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/?sh=2ad6ad3f7da5

He also emphasised that applications such as TikTok “screams out with national security concerns”.[18]

### *Outcome*

Because of a series of legal challenges and the new administration coming into power, the national ban on TikTok or the involvement of the US companies to manage the application was not enforced.[19]

However, under Biden’s new administration, the US approved an unprecedented ban on the use of TikTok on federal government devices due to the national security concerns raised previously. The order commanded governmental offices to plan and execute “standards and processes for all government employees to remove the app from their phones”.[20] These measures were imposed to avoid any filtration of sensitive information being collected by the Chinese government.

The US congress is considering a nationwide prohibition on apps subject to Chinese government control. Nevertheless, the Committee on Foreign Investment in the United States has ordered ByteDance to “sell TikTok or face a ban in the United States.” TikTok company, on the other hand, has reinforced their willingness to comply with any condition imposed by the US government to keep operating in the country. They have defended themselves by stating that a business sellout would not “address national security concerns because it wouldn’t put any new restrictions around access to the app’s data”.[21]

[18] Martina, M., & Zengerle, P. (2023, March 9). FBI chief says TikTok 'screams' of US national security concerns. Retrieved from Reuters: https://www.reuters.com/technology/fbi-chief-says-tiktok-screams-us-national-security-concerns-2023-03-08/

[19] BBC. (2021, June 9). Donald Trump-era ban on TikTok dropped by Joe Biden. Retrieved from BBC: https://www.bbc.co.uk/news/technology-57413227

[20] Bhuiyan, J. (2022, December 31). Why did the US just ban TikTok from government-issued cellphone? Retrieved from The Guardian: https://www.theguardian.com/technology/2022/dec/30/explainer-us-congress-tiktok-ban

[21] Healey, J. (2023, March 16). The Biden administration’s threat to ban TikTok: Here’s what you should know . Retrieved from Los Angeles Times: https://www.latimes.com/business/story/2023-03-16/the-biden-administrations-threat-to-ban-tiktok-heres-what-you-should-know

## Case 3: The return of Anonymous during the Russian war against Ukraine — 2022

### *Actors Involved*

- Anonymous - collective hacktivist
- Government of the Russian Federation and President Vladimir Putin
- Private sector: telecommunications, space oil and gas.
- IT Army - Ukraine cyber army initiative
- Other groups of hackers

### *Actions*

Anonymous joins the conflict between Russia and Ukraine by declaring a "cyber war" against the government of Russia for launching the 'special operation' invasion.

Anonymous claimed the responsibility for several cyber-attacks, coded Operation Russia #OpRussia, which consisted of:[22]

- Hacking into databases and posting leaked information from the Central Bank of Russia, the space agency Roscosmos, oil and gas, broadcaster, IT companies, law firms and more.
- Defacing Kremlin websites and blocking Belarusian websites.
- Disrupting internet connectivity at the St. Petersburg International Economic Forum which delayed Vladimir Putin's keynote speech by some 100 minutes.
- Targeting and blocking companies that continue to do business in Russia.
- Training of people to launch DDoS attacks and mask their identities whilst providing cybersecurity assistance to Ukraine.
- Hijacking media and streaming services.

[22] Pitrelli, M. (2022, July 28). Hacktivist group Anonymous is using six top techniques to 'embarras'Russia. Retrieved from CNBC: https://www.cnbc.com/2022/07/28/how-is-anonymous-attacking-russia-the-top-six-ways-ranked-.html

- Directly hacking to Russians citizens to send messages anti-war and pro-Ukrainian via calls, emails, text messages and Russian social networking site VK.

### *Affected Layers of the Internet*

All layers: physical, platform, information and people.

### *Power Relationships*

Some telecommunications such as RT, confirmed the cyber-attacks received and attributed them to Anonymous while claiming most of them were launched from millions of devices within the US.[23]

Ukraine's deputy prime minister, and minister for digital transformation, celebrated Anonymous intervention in favour of its country[24].

Following Anonymous lead, the Ukraine's minister decided to coordinate a cyber army, IT Army, of civil volunteers to join the cyber front against Russia. Cyber volunteers were centrally directed with given instructions via Telegram, while belonging to different parts across the world. [25]This army was mainly tasked with taking down Russian disinformation from the web and targeting Russian infrastructure.

Professional hackers from Ukraine have been leaking "whatever sensitive information they can find against Russian targets."[26]

Another hacking group that merged with Anonymous was Squad 303, a Polish hacker group. According to members of this hacking group, they have

[23] Milmo, D. (2022, February 27). Anonymous: The hacker collective that has declared cyberwar on Russia. Retrieved from The Guardian: https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia

[24] RTVE. (2022, February 26). Anonymous declara la ciberguerra a Rusia y a Putin por Ucrania. Retrieved from RTVE: https://www.rtve.es/noticias/20220226/anonymous-declara-ciberguerra-rusia-ucrania/2297941.shtml

[25] Faife, C. (2022, March 11). In Ukraine, hacktivists fight back with data leaks. Retrieved from The Verge: https://www.theverge.com/2022/3/11/22968049/anonymous-hacks-ukraine-russia-cybercrime-danger

[26] See Faife (2022, March 11)

previously collaborated with Anonymous, although they decided, during the period of the war, to be considered part of anonymous and not separate partners anymore. The hacker group also built a website to allow "members of the public to send text messages to random Russian phone numbers, telling them the truth about the war. They claim to have facilitated more than 20 million SMS and WhatsApp messages."[27]

A pro-Kremlin hacker collective by the name of Killnet entered a cyber feud with Anonymous due their cyber-attacks against Russia. Both collective groups remained at odds by taking opposing political sides, although this 'fight' did not have greater consequences outside the cyber realm.[28] "Killnet's aim is to make Europeans pay for their unequivocal support of Ukraine and punish Western governments for their anti-Russian sentiment."[29] Despite their vocal support for Russia, this hacker collective did not pose a greater threat to other hackers collective fighting in support of Ukraine.

### *Outcome*

A cyber retaliation by Russia or any escalation in cyber offence operations was expected, such as the NotPetya malware assault in 2017, yet the impact has been minimal. Nevertheless, there were attempts of other type of cyber tactics such as using wiper attacks.[30]

Despite the scale of the invasion, known hacker groups associated to Russia such as Fancy Bears, have not conducted any massive cyber offensive operation. Many speculations were proposed but no agreed conclusion has been made.[31]

[27] Tidy, J. (2022, March 20). Anonymous: How hackers are trying to undermine Putin. Retrieved from BBC: https://www.bbc.co.uk/news/technology-60784526

[28] Uchill, J. (2022, 23 May). *Cyber feud between Anonymous and Killnet groups unlikely to affect others*. Retrieved from SCMedia: https://www.scmagazine.com/analysis/cyber-feud-between-anonymous-and-killnet-groups-unlikely-to-affect-others

[29] Roussi, A. (2022, September 9). Meet Killnet, Russia's hacking patriots plaguing Europe . Retrieved from Politico: https://www.politico.eu/article/meet-killnet-russias-hacking-patriots-plaguing-europe/

[30] See Milmo (2022, February 27).

[31] Marks, J. (2022, March 3). 11 reasons we haven't seen big Russian cyberattacks yet. Retrieved from The Washington Post: https://www.washingtonpost.com/politics/2022/03/03/11-reasons-we-havent-seen-big-russian-

Although, Anonymous has threatened Putin directly with revealing information that he has been concealing for years which would completely expose him and his corrupt officials.[32] There have been no significant leaks, nor any of the attacks perpetrated by the collective were sophisticated enough for these threats to become a reality.

Increased hacktivism activities by a variety of groups since the start the invasion have been difficult to trace. This has also meant that there is no confirmed number of groups acting under the Anonymous name, nor a precision of all the cyber-attacks being perpetrated by the collective. In addition, some of the claims made by Anonymous have been cleared as false while others were difficult to confirm. In addition, there was the issue of some of the cyber-attacks proclaimed in 'support' of Ukraine could have other motivations behind such as for performing cybercrime.[33]

## Case 4: Facebook (Meta) communication conflict with Australia — 2021

### *Actors Involved*

- Private sector - technology: Facebook (Meta)
- Private sector - media
- The Australian Government
- Australian citizens
- International community

### *Actions*

A planned law (called News Media and Digital Platforms Mandatory Bargaining Code) caused a dispute between Facebook and the Australian government. This law would force Big Tech companies such as Google and

cyberattacks-yet/

[32] See RTVE (2022, February 26).

[33] See Faife (2022, March 11)

Facebook to pay publishers for news content in Australia. An action perceived as 'fair' from the Australian government and to protect the media industry. In addition, this would be the first law that directly targeted Big Tech companies seeking to "address the media's loss of advertising revenue to US tech firms."[34]

In response to the proposed law, Facebook decided to block news content from its platform by restricting "publishers and people in Australia from sharing or viewing Australian and international news content." Facebook also claimed that the law "fundamentally misunderstands the relationship between our platform and publishers who use it to share news content". On the other hand, Google decided to form a partnership with an Australian media company.[35]

### *Affected Layers of the Internet*

Platform, information and people layers

### *Power Relationships*

Facebook response, in contrast to Google's actions, showed Big Tech firms reservations regarding "paying news publishers for their right to link to their content in news feeds or search results[36]". Furthermore, Facebook justified their decision commenting that they were put in a difficult position having "to comply with a law that ignores the realities of this relationship or stop allowing news content on our services in Australia." Additionally, they justified their attitude in relation to other tech firms by stating that "our

[34] BBC. (2021, February 18). Australia news code: What's this row with Facebook and Google all about? Retrieved from BBC: https://www.bbc.co.uk/news/world-australia-56107028

[35] Easton, W. (2021, February 17). Changes to sharing and viewing news on Facebook in Australia. Retrieved from Meta: https://about.fb.com/news/2021/02/changes-to-sharing-and-viewing-news-on-facebook-in-australia/

[36] Shead, S. (2021, February 19). It will 'annoy a huge group of the population': How Australians have responded to Facebook's news ban. Retrieved from CNBC: https://www.cnbc.com/2021/02/19/australians-respond-to-facebooks-news-ban.html

platforms have fundamentally different relationships with news".[37]

Reactions from the Australian government bodies described Facebook's statement as "bullying" "staggeringly irresponsible" and "the worst type of corporate culture".[38] Besides they claimed that Facebook was levering their power in controlling information and news content in their platform, and that this demonstrated an act of power to oppose to the law. In return, Facebook commented that the Australian government "must take into account whether a digital platform [that] has made a significant contribution to the sustainability of the Australian news industry"[39] should succumb to such law.

Response among the Australian citizens and users was divided between those that were indifferent, and those that showed angry reactions. The latter also provoked the #deletefacebook hashtag to trend in the Twitter platform to express their discontent with Facebook. As a collateral effect, "when removing news pages from its platform, Facebook also inadvertently pulled pages for dozens of charities, state health organizations, small businesses, and a weather bureau."[40]

Other states from the world reacted to the move done by Facebook with criticisms towards the company. Many cited that the removal of trusted news media organisations would allow misinformation and conspiracy theories to thrive among the absence of factual information.[41]

### *Outcome*

The Australian law intended to address longstanding "concerns about the market dominance of tech firms over media organisations"[42]. Which, if being passed would have set a precedent for other states to follow suit.

[37] BBC. (2021, February 18b). Facebook Australia news ban 'bullying', says UK MP. Retrieved from BBC: https://www.bbc.co.uk/news/uk-56117946

[38] See BBC (2021, February 18b).

[39] Thornton, C., & Toh, M. (2021, February 25). Australia passes new law requiring Facebook and Google to pay for news. Retrieved from CNN Buisness: https://edition.cnn.com/2021/02/24/media/australia-media-legislation-facebook-intl-hnk/index.html

[40] BBC. (2021, February 18c). *Facebook Australia: Tech giant faces growing criticism over news ban*. Retrieved from BBC: https://www.bbc.co.uk/news/world-australia-56116738

[41] See BBC (2021, February 18c).

[42] See BBC (2021, February 18a).

After a week of the dispute, the Australian government and Facebook reached an agreement to change the landmark media bargaining code. The changes reflected that Facebook would not be accountable under the law "if the company can demonstrate it has signed enough deals with media outlets to pay them for content."[43] In Facebook behalf, they published an updated statement that celebrated the agreement reached between both parties. Adding that the new code demonstrates: "the value our platform provides to publishers relative to the value we receive from them" and that "we can now work to further our investment in public interest journalism".[44]

## A cyber international level of analysis: Net state-to-state relations

The preliminary cases presented in this section portrayed a range of actors, scope and outcomes to assess the concept of Net States as a phenomenon outside the traditional framework of state-to-state relations that governs international security. Some common conclusions were categorised in accordance to Gamero-Garrido's (2014) study consisting of:

### *(a) Actors*

The current cyber-political scenario includes a few cyber entities that have demonstrated the power and control equivalent to that of states.

- In all the majority of the cases Net states have taken advantage of their power and capabilities to initiate conflicts against states. This is with the exception of the second case in which the Net state took a defensive approach.
- In all cases it can be perceived that the number of actors involved is quite varied, having representation from the public and private sectors.

[43] Meade, A., Josh, T., & Hurst, D. (2021, February 23). Facebook reverses Australia news ban after governmrnt make media code amendmests. Retrieved from The Guardian: https://www.theguardian.com/media/2021/feb/23/facebook-reverses-australia-news-ban-after-government-makes-media-code-amendments

In some cases, the industries involved represented critical infrastructure, while in others the media acted as a mediator factor. In addition, civilians had a minor role in the support of either Net states or states.

- The involvement of certain actors, however, did not always resulted in active participation on the conflict or leverage of power.
- The presence of collaboration or cooperation between states and Net states was fairly absent. Except in the last case, and to some extent the third case in which hacker groups collaborated with Anonymous.

### *(b) Socio-Political Context*

The cases analysed different situations of recent events that intended to capture political interactions, decision-making dynamics and initiation or escalation of conflicts at an international level. From the results:

- In all cases, disputes involved power distribution and political motivations.
- From the cases presented, two were related to hacktivism, one to cyber espionage and the last to cyber sovereignty.
- Cases involving Big Tech firms were an example of conflict that was already occurring in the physical realm. However, the cases on hacktivism involves cyber conflicts that crossed into the physical sphere.

### *(c) Outcome and Damage*

The majority of the cases demonstrated little significant consequences with the duration of the conflicts being rather fleeting. Although, the scale and scope of cyber-attacks used in some of the conflict had a large-scale impact, reactions from states were minimal.

[44] See Easton (2021, February 17).

- The hacktivism cases involved little if no governmental response to the cyber-attacks perpetrated against them. In the case of Guacamaya, despite the large-scale severity of the attacks involving a whole region, the set of measures taken only involved patching the technical vulnerabilities. No revision to their cyber strategies policies were made, nor any other measures taken.
- Due to the geopolitical motivations embedded in the TikTok case, the conflict is still on going. Besides, the buyout talks did not have any resolute outcome despite willingness demonstrated by TikTok to follow the conditions imposed by the US.
- Facebook's retaliation against the passing of the revised law leveraged pressure onto the Australian government as there was no precedent for the conflict. However, the agreement reached meant that such behaviour displayed by the Tech giant can be repeated in the future.

### *(d) Accountability*

The uncertainty surrounding identity and location within cyberspace can obscure the attribution of cyber-attacks perpetrated against an entity. This in return makes accountability difficult to open an investigation or press charges.

- In the first hacktivism case, accountability rested mainly in the hands of the private industry rather than on the actual hacktivists. Therefore, no formal investigations were conducted to prosecute the group despite the amount of classified information collected.
- In the Anonymous case, attribution of the attacks were claimed since the very beginning. Some representatives from the industries affected also admitted to the attacks and blamed Anonymous. However, the Russian government did not take any counteroffensive.
- In the two Big Tech cases, both parties involved in the main conflict accused the other for lacking in accountability for their attitudes. In the case of TikTok, the conflict involved lawsuits, and the main issue has not been resolved. In the case of Facebook, an intervention in the form

of negotiation talks was necessary to reach a formal agreement.

# Discussion

"If the system were transformed, international politics would no longer be international politics, and the past would no longer serve as a guide to the future"[45]

The present dissertation was undertaken to investigate the novel phenomenon designated as Net state and evaluate its power and impact in the international security landscape. Adopting a neorealism theoretical framework, predominant paradigm in IR, it also attempted to determine how the integration of a cyber reality into the international politics can alter traditional conceptions of security. Divided into two main parts, the general results of both studies conducted suggests that: (a) Net states have theoretical implications to be considered as a unit of level under the same conceptual standards as traditional states, (b) and predicts that the cyber-physical revolution has the possibility to exacerbate interactions between states and Net states resulting in hybrid conflicts.

In the first part of the dissertation, findings from the cases illustrated the relevance of Net states for the field of international security through a series of challenges posed to sovereign states. Firstly, and most importantly, Net states threatens traditional forms of governance and authority in cyberspace (Rizvi, 2018). As a volatile and dynamic domain consisting in interconnected networks and human interactions. There is a plethora of actors that have taken advantage of the characteristics of cyberspace to pursue digital disruption (Nye, 2022). However, only a handful have achieved greater influence over the Internet user base while taking control of the physical aspects of cyberspace. The most representative case being Big Tech, which: possess and control major technical components in cyberspace, have their own security apparatuses, are self-governed by norms and policies, and even have representatives to take on business and diplomatic negotiations (Wichowski, 2017). The cases of WikiLeaks and Anonymous, in addition, represent alternative forms of organisations. Promoting social causes by influencing the global population of cyberspace and having greater knowledge about the mechanisms to ensure smooth operations on the Internet (Sorell, 2015).

Secondly, there is the issue with Net states impact on public opinion and political discourse. As mentioned, the influence of Net states on the Internet community is significant. Through the digital platforms of Big Tech, information flows and connects many people in the world, collecting personal data for later ad customisation and algorithm governance (Kreps, 2020). Anonymous and WikiLeaks can influence ideologies on people and use their platforms to sow discord and polarise nation states. Thirdly, Net states might become threats to national security if they engage in actions that might be perceived as dangerous for states. For instance, Net states such as WikiLeaks and Anonymous have been labelled as threats for national security due to their malicious practices that involve hacking, leaks of sensitive information and cyber-attacks (Benkler, 2011). Although Big Tech have not engaged in these negative practices, they have also generated national security concerns in some occasions (Chachko, 2021). Such as, allowing rampant misinformation in their platforms and the collection of personal data that could be breached or used for espionage and surveillance (Shull & Hilt, 2021). Thus, Net states' characteristics show an equal level of power and authority (if not greater) than nation states within an anarchic cyber-international system.

Furthermore, form the application of a neorealist framework, it can be said that Net states sustainability over the years is similar to the concept of self-help. In this regard, Net states have shown attitudes towards self-preservation by ensuring the pursuit of their belief-driven agendas and interests; as well as being responsible to leverage the necessary security safeguards to protect their integrity (Choucri & Clark, 2019). Hence, findings from this study confront the neorealist assumption that states are the only constitute units in the international system (Waltz, 2003). The existence of

[45] See Waltz (2000, p. 6)

cyberspace as a parallel reality to that of the physical world implies that traditional states will have their counterparts within this new reality, as argued in the form of Net states. Therefore, in a cyber-international system the units of study should be states *and* Net states alike which poses a conceptual challenge to IR paradigms.

In order to explore the cyber-international system influence on states' interactions with Net states, the second part of the dissertation proposed the following hypothesis: Net states retention of cyber power will challenge nation states' behaviours in cyberspace, hence, increasing the likelihood of conflicts impacting the real and cyber realms. Results from the cases narrated, however, did not fully corroborated this. Although, it did partially support the fact that Net states were perceived in general as sovereignty threats (Koley, 2017), this caused some tensions that did not escalate into major conflicts. Despite this, in the majority of the cases where Net states took an offensive approach, states did not launch any counteroffensive operation, nor decided to take further actions apart from legal methods. Only one of the cases, namely US against TikTok showed a prevalent and unresolved conflict deeply rooted on geopolitics. An interesting finding was in relation to the Guacamaya's case. Because not only can be considered one of the major cyber-attacks conducted at a regional level, but also because the states did not follow suit against the collective. In addition, no revision to their cyber security strategies was made, and even in the case of Mexico, the president himself dismissed the national security consequences of releasing confidential governmental information.

In a similar sentiment, despite the scale and scope of cyber-attacks perpetrated by Anonymous against the Russian government and many other of its critical industries – no counter offensive was proceeded. Even when attribution was not an issue in this conflict, as Anonymous claimed responsibility for the attacks that were later verified. This included some industries representatives that also confirmed the malicious attacks. However, it is necessary to comment that the intensity of the cyber-attacks only lasted for a few months. By the end of the year, there has not been major publications about the progress of the operation. Therefore, the offensive operation was rather short-lived despite the grandiose declaration of launching a ‘cyber war’. In addition, at the time, many other hacker collectives were collaborating with Anonymous which might have gradually dissolved causing the cease of cyber-attacks, and a failure of the operation. The example of Facebook blocking news media outlets in its platform, however, was regarded by the international community as a cause of great controversy. Despite this, Facebook remained inflexible in their standing towards the passing of the bill, which pressured the Australian government into making further modifications. Although eventually an agreement was reached, it created a new precedent for further similar future behaviour, and also for other Big Tech firms to do the same.

From a theoretical perspective, Net states leverage of their cyber power and capabilities reflect a change in the balance of states relations in the international system (Klimburg, 2011a). Findings from the second study implies that, although, there were few cases of serious cyber conflicts; there were also some instances of cooperation with other non-state actors or policy-making collaboration. This, further, corroborates the need of an Internet governance based on a multistakeholder structure that integrates states and Net states alike (Shen, 2016). Moreover, by looking at the cases involving Big Tech firms of US and China. It can be observed that while Facebook acted as a standalone Net state, TikTok’s identity on the other hand, was predominately shadowed by the Chinese government. Therefore, this would support the argument that some Net states can actually be leveraged as proxy organisations by authoritarian governments as a distinctive type of Net states (Harvey & Moore, 2022; Klimburg, 2011a). The different reactions and measures (or lack of) can be associated to literature on cyber security strategies having little impact in practice or not being actionable enough (Shafqat & Masood, 2016).

Overall, the advent of cyberspace has brought some transnational changes to the international system. Within an integrated cyber-IR context, the cyberspace has generated cyber sovereign entities that are trying to survive under the organising principle of the international (cyber) system. This indicates possible repercussions to the security landscape in cyberspace as Net states keep developing their capabilities and expanding their cyber power (Choucri & Clark, 2019). At an international level, this seemly power imbalance between Net states and traditional states is starting to cause some minor frictions that could lead into future cyber conflicts, disrupting the equilibrium of the international-political system. In allusion to Waltz (2000) quote at the beginning of this section, this dissertation argues that a cyber-international relations framework would still incorporate an anarchic organising principle. This would include concepts such as uncertainty, balance of power, security dilemma, authority and capabilities. However, the theory needs a conceptual expansion concerning the units of level analysis, to acknowledge the inclusion of the new key entities of cyberspace – namely Net states. As this is what the cyberspace has fundamentally changed, the interaction from state-to-state to Net state-to-state. Thus, in response to the quote, although the system did not undergo a major transformation, in the future, the international politics must evolve to become integrated with the new reality called cyber.

## Limitations

The purpose of this dissertation was to empirically examine the phenomenon of Net States within the framework of international security studies by applying an abduction approach. Therefore, the findings presented in this study must be interpreted with caution as current literature and data available on this phenomenon is still underdeveloped. In addition, the used terminology 'Net States' to refer to such phenomenon presented as a thesis was deemed as the most appropriate, although this might be refuted. Some additional complications that this dissertation might have been unable to discuss in sufficient depth concerns the application of the concept Net state to other theoretical approaches in IR such as contructivism or liberalism. The case studies used in the second part for evaluation attempted to provide a variety of examples from different international regions. However, the focus might manifest a 'Western' perspective and cannot be claimed to be a truly global undertaking. This dissertation is not fit for the purpose of establishing a theoretical framework and requires further rigorous empirical research that can be complemented by quantitative methods. The overall approach was directed at expanding literature on the topic and uniform theoretical enquiries on non-state entities, and their strategical implications. Hence, it is important to note that Net States continue to be a relatively new phenomenon, limited tested and without standardised conventions or procedures. Therefore, their impact on international security is not yet clear, which would ultimately depend on how the concept of Net States evolve and their integration into the international system.

## Future Research

Cyberspace as a fast-paced evolving phenomenon continues to be a challenging topic to research in relation to international security. Although literature on the topic has been growing in recent years, many conceptual frameworks have been formulated on the categorisation of non-state actors and entities. However, the absence of a unified and comprehensive theoretical framework that understand cyberspace influence in the international-political community remains (Choucri & Clark, 2019). Therefore, with the introduction of new technological advancements such as artificial intelligence and Web 3.0, there is an urgent academic need to develop better practice standards and metrics to measure phenomena in cyberspace (De Gregorio & Radu, 2022). Of particular relevance, future studies could benefit from researching the concept of Net states by applying quantitative or statistical methods to increase replication and validity of findings. Thus, taking into consideration some of these recommendations would advance the field of cyber and international relations while applying rigorous scientific methods.

## Conclusion

The 4th Industry Revolution signifies an era in which the merging of the physical and cyber realities will bring profound transformations to the international community. For the politics world, the cyberspace represents an expanding conceptual medium of decentralised interconnected networks and social interactions, complex and dynamic, reigned by the flow of information. In this domain, individuals and entities build and define the future, for the better by sharing values and goals or for the worse by causing disruption and havoc. Therefore, as states enter the cyberspace to assert their sovereignty, the increasing diversification of non-state actors will pose threats and challenges to states' ability to govern and protect their national security. However, current international relations theories such as traditional realism do not consider influential non-state groups or entities as analogous to states in capacity to transform the international-political system. In order to understand this phenomenon, this dissertation proposed Net states as a conceptual unit of analysis equivalent to states within an anarchic international system. Furthermore, neorealism assumptions were discussed to comprehend interaction dynamics between Net states and nation states, and how this can affect the distribution of cyber power within cyberspace. Theoretical implications from the results suggest the idea of Net states becoming equally powerful as sovereign states at the international level is a reality driven by the cyberspace. Thus, from the narrative findings, this dissertation has provided a deeper insight into the topic of cyber-international relations and the strategical implications that Net states could have for security in the cyber-physical age.

# Bibliography

Al Jazeera. (2020, December 17). *What is the Arab Spring, and how did it start?* Retrieved July 18, 2023, from AL JAZEERA: https://www.aljazeera.com/news/2020/12/17/what-is-the-arab-spring-and-how-did-it-start

Anonymous. (2020). *10 prolific historical Anonymous Operations*. Retrieved July 18, 2023, from We Are Anonymous: https://iamanonymous.com/10-prolific-historical-anonymous-operations/

Anonymous. (n.d.). *About Anonymous*. Retrieved July 18, 2023, from Anonymous Hackers: https://www.anonymoushackers.net/anonymous-history/

AnonymousNetherlands. (2011, August 4). *Anonymous Original Message to Scientology* [Video]. Youtube: https://www.youtube.com/watch?v=qlJ-Yb0j3ck

Azmi, R., Tibben, W., & Win, K. T. (2016). Motives behind cyber security strategy development: A literature review of national cyber security strategy. *Australasian Conference on Information Systems* (pp. 1-12). Wollongong: Australasian Conference on Information Systems.

Baker-White, E. (2022, December 22). *TikTok Spied On Forbes Journalists*. Retrieved from Forbes: https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/?sh=2ad6ad3f7da5

Barlow, J. P. (1996). *A declaration of the independence of cyberspace*. Retrieved from Electronic Frontier Foundation: https://www.eff.org/cyberspace-independence

Brainard, L. A., & Brinkerhoff, J. M. (2004). Lost in Cyberspace: Shedding Light on the Dark Matter of Grassroots Organizations. *Nonprofit and Voluntary Sector Quarterly, 33*(3), 32-53. doi: 10.1177/0899764004265436

BBC. (2020a, August 7). *TikTok threatens legal action against Trump US ban*. Retrieved from BBC: https://www.bbc.co.uk/news/business-53660860

BBC. (2020b, August 7). *TikTok: President Trump signs orders to ban it in the US within 45 days*. Retrieved from BBC: https://www.bbc.co.uk/newsround/53620689

BBC. (2021, February 18a). *Australia news code: What’s this row with Facebook and Google all about?* Retrieved from BBC: https://www.bbc.co.uk/news/world-australia-56107028

BBC. (2021, February 18b). *Facebook Australia news ban 'bullying', says UK MP*. Retrieved from BBC: https://www.bbc.co.uk/news/uk-56117946

BBC. (2021, February 18c). *Facebook Australia: Tech giant faces growing criticism over news ban*. Retrieved from BBC.

https://www.bbc.co.uk/news/world-australia-56116738

BBC. (2021, June 9). *Donald Trump-era ban on TikTok dropped by Joe Biden*. Retrieved from BBC: https://www.bbc.co.uk/news/technology-57413227

BBC. (2022, September 30). *Qué se sabe de Guacamaya, el cibergrupo clandestino que reveló los problemas de salud de AMLO y ha robado secretos a varios de países de América Latina*. Retrieved from BBC: https://www.bbc.com/mundo/noticias-america-latina-63098421

Bhuiyan, J. (2022, December 31). *Why did the US just ban TikTok from government-issued cellphone? Retrieved from The Guardian*: https://www.theguardian.com/technology/2022/dec/30/explainer-us-congress-tiktok-ban

Branscomb, A. W. (1995). Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces. *The Yale Law Journal, 104*(7), 1639–1679. doi:10.2307/797027

Bronk, C. (2012). *A governance switchboard: Scalability issues in international cyber policymaking.* Toronto: Baker Institute for Public Policy, Rice University.

Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies, 21*(5), 594–613. doi:10.1177/1367549417751151

Bussell, J. (2013, March 12). *Cyberspace*. Retrieved from Encyclopedia Britannica: https://www.britannica.com/topic/cyberspace

Bussolati, N. (2015). The Rise of Non-State Actors in Cyberwarfare. In J. D. Ohlin, K. Govern, & C. Finkelstein, *Cyber War: Law and Ethics for Virtual Conflicts* (pp. 102–126). Oxford: Oxford Academic.

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. Retrieved June 23, 2023, from The Guardian: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs, 92*(1), 43-62.

Caton, J. L. (2013). Exploring the prudent limits of automated cyber attack. *5th International Conference on Cyber Conflict (CYCON 2013)* (pp. 1-16). Tallinn: NATO CCD COE Publications.

Cavelty, M. D. (2015a). Cyber-security. In A. Collins, *Contemporary Security Studies* (4th ed., pp. 400-416). Oxford: Oxford University Press.

Cavelty, M. D. (2015b). The normalization of cyber-international relations. In M. D. Cavelty, J. Grätz, M. Haas, O. Thränert, & M. Zapfe (Eds.), *Strategic Trends 2015: Key Developments in Global Affairs* (pp. 81-98). Zurich: Center for Security Studies, ETH Zurich.

Chachko, E. (2021). National security by platform. *Stanford Technology Law Review*, *25*(1), 55-140.

Chandel, S., Jingji, Z., Yunnan, Y., Jingyao, S., & Zhipeng, Z. (2019). The golden shield project of China: A decade later—An in-depth study of the great firewall. *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 111-119. doi:10.1109/CyberC.2019.00027

Choucri, N., & Clark, D. D. (2019). *International Relations in the Cyber Age: The Co-Evolution Dilemma*. Cambridge, MA: The MIT Press. doi:10.7551/mitpress/11334.001.0001

Clark, G. (2019, June 11). *Regulation for the Fourth Industrial Revolution*. Retrieved from GOV.UK: https://www.gov.uk/government/publications/regulation-for-the-fourth-industrial-revolution/regulation-for-the-fourth-industrial-revolution

Craig, A., & Valeriano, B. (2016). Conceptualising cyber arms races. *8th international conference on cyber conflict (CyCon)* (pp. 141-158). Tallinn: NATO CCD COE Publications.

Crowther, G. A. (2017). The Cyber Domain. *The Cyber Defense Review*, 63-78.

De Gregorio, G., & Radu, R. (2022). Digital constitutionalism in the new era of Internet governance. *International Journal of Law and Information Technology, 30*(1), 68–87. doi:10.1093/ijlit/eaac004

Deibert, R. J. (2013, October 16). *Bounding cyber power: Escalation and restraint in global cyberspace.* Retrieved from Centre for International Governance Innovation: https://www.cigionline.org/sites/default/files/no6_2.pdf

Diaz, R. (2022, September 30). *Guacamaya Hackers: ¿Cómo lograron hackear a la Sedena? Esta es la increíble respuesta*. Retrieved from Sdpnoticia: https://www.sdpnoticias.com/mexico/guacamaya-hackers-como-lograron-hackear-a-la-sedena-esta-es-la-increible-respuesta/

Doyle, B. (2019). The Whole-of-Nation and Whole-of-Government approaches in action. *InterAgency Journal, 10*(1), 105-122. Retrieved from The Simons Center.

Easton, W. (2021, February 17). *Changes to sharing and viewing news on Facebook in Australia*. Retrieved from Meta: https://about.fb.com/news/2021/02/changes-to-sharing-and-viewing-news-on-facebook-in-australia/

Eden, L. (2018). The Fourth Industrial Revolution: Seven lessons from the past. In R. van Tulder, A. Verbeke, & L. Piscitello, *International Business in the Information and Digital Age* (pp. 15-35). Bingley: Emerald Publishing Limited.

Eordogh, F. (2014, January 22). *The video that made Anonymous*. Retrieved July 18, 2023, from VICE: https://www.vice.com/en/article/78x9w9/the-video-that-made-anonymous

Espinosa Robledo, N. (2023, January 8). *Grupo Guacamaya hackeó la Agencia Nacional de Hidrocarburos y empresas del sector petrolero*. Retrieved from El Colombiano:

https://www.elcolombiano.com/colombia/hackeo-a-agencia-nacional-de-hidrocarburos-de-colombia-BH19780540

Faesen, L., Torossian, B., Mayhew, E., & Zensus, C. (2020). *Conflict in cyberspace: Parsing the threats and the state of international order in cyberspace*. Retrieved July 20, 2023, from Strategic Monitor 2019: https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/conflict-in-cyberspace/

Faife, C. (2022, March 11). *In Ukraine, hacktivists fight back with data leaks*. Retrieved from The Verge: https://www.theverge.com/2022/3/11/22968049/anonymous-hacks-ukraine-russia-cybercrime-danger

Fukuyama, F., Richman, B., & Goel, A. (2021). How to Save Democracy from Technology: Ending Big Tech's Information Monopoly. *Foreign Affairs, 100*(1), 98-110.

Gamero-Garrido, A. (2014). Cyber conflicts in international relations: Framework and case studies. *MIT Political Science Department*, 1-95.

Gibson, W. (1984). *Neuromancer.* New York: Ace Books.

Gillham, P. F., Edwards, B., & Noakes, J. A. (2013). Strategic incapacitation and the policing of Occupy Wall Street protests in New York City, 2011. *Sociology, 23*(1), 81-102. doi:10.1080/10439463.2012.727607

Grosby, S. (1997). The Decline of the National State?. *Sociological Forum, 12*(2), 331–338.

Gross, J. R. (2016). Hack and be hacked: framework for the United States to respond to non-state actors in cyberspace. *California Western International Law Journal, 46*(2), 109-146.

Gu, H. (2023). Data, Big Tech, and the New Concept of Sovereignty. *Journal of Chinese political science*, 1–22. Advance online publication. doi:10.1007/s11366-023-09855-1

Guacamaya. (n.d.). *No somos defensores de la vida, somos vida!* Retrieved from https://enlacehacktivista.org/comunicado_guacamaya4.txt

Hall, R., & Biersteker, T. (2002). *The Emergence of Private Authority in Global Governance*. Cambridge: Cambridge University Press. doi:10.1017/CBO9780511491238

Harvey, C. J. (2021). *Mapping the Net State: Towards a Framework for Cyber Statecraft*. Retrieved from https://homebrewdrafts.wordpress.com/thesis/

Harvey, C. J., & Moore, C. L. (2022). The client net state: Trajectories of state control over cyberspace. *Policy & Internet*, 1– 19.

Healey, J. (2011, Decemeber 14). *The five futures of cyber conflict and cooperation.* Retrieved from Atlantic Council: https://www.atlanticcouncil.org/wp-content/uploads/2011/12/121311_ACUS_FiveCyberFutures.pdf

Healey, J. (2023, March 16). *The Biden administration's threat to ban TikTok: Here's what you should know* . Retrieved from Los Angeles Times: https://www.latimes.com/business/story/2023-03-16/the-biden-adminis trations-threat-to-ban-tiktok-heres-what-you-should-know

Hennig, B. D. (2021). In Focus: Trump Tweets: Power and the Global Politics of Social Media. *Political Insight, 12*(1), 20–21. doi:10.1177/20419058211000998

Hiller, J. S., & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law & Security Review, 29*(3), 236-245. doi:10.1016/j.clsr.2013.03.003

Hindman, E. B., & Thomas, R. J. (2014). When old and new media collide: The case of WikiLeaks. *New Media & Society, 16*(4), 541–558. https://doi.org/10.1177/1461444813489504

HISTORY. (2019, October 21). *WikiLeaks publishes the first documents leaked by Chelsea Manning*. Retrieved July 19, 2023, from HISTORY: https://www.history.com/this-day-in-history/wikileaks-publishes-first-documents-leaked-by-chelsea-manning

Hobbs, A., (2021). Trump’s expulsion from social media: When is it time to ban an account?. In *Sage Business Cases*. SAGE Publications, Ltd., doi:10.4135/9781529775181

Ibáñez Múñoz, J. (2021). The normative dimension of platform governance: Big Tech and digital platforms as normative actors. *Spanish Yearbook of International Law, 25*, 128–137. doi:10.17103/sybil.25.8

International Business Times. (2011). *Anonymous Hackers Demand 'Social Justice' with Occupy Wall Street Protest*. Retrieved July 18, 2023, from International Business Times: https://www.ibtimes.co.uk/anonymous-hackers-demand-social-justice-with-operation-occupy-wall-street-hack-206540

Johnson, D. R., & Post, D. (1996). Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review, 48*(5), 1367–1402. doi:10.2307/1229390

Jordan, T. (2015). Hacktivism: Operation Tunisia, Modular Tactics and Information Activism. *In Information Politics: Liberation and Exploitation in the Digital Society* (pp. 176–191). Pluto Press. doi:10.2307/j.ctt183p2xf.14

Junio, T. J. (2013). How probable is cyber war? Bringing IR theory back In to the cyber conflict debate. *Journal of Strategic Studies, 36*(1), 125-133. doi:10.1080/01402390.2012.739561

Karagiannopoulos, V. (2021, June 29). *A decade since ‘the year of the hacktivist’, online protests look set to return*. Retrieved from The Conversation: https://theconversation.com/a-decade-since-the-year-of-the-hacktivist-online-protests-look-set-to-return-163329

Kazmi, A. (2011). *How Anonymous emerged to Occupy Wall Street*. Retrieved July 18, 2023, from The Guardian: https://www.theguardian.com/commentisfree/cifamerica/2011/sep/27/occupy-wall-street-anonymous

Kelly, B. B. (2012). Investing in a centralized cybersecurity infrastructure:

Why hacktivism can and should influence cybersecurity reform. *Boston University Law Review, 92*, 1663-1711.

Khan, A. (1992). The extinction of nation-states. *American University International Law Review, 7*(2), 197-234.

Klimburg, A. (2011a). Mobilising cyber power. *Survival, 53*(1), 41-60. doi:10.1080/00396338.2011.555595

Klimburg, A. (2011b). The Whole of Nation in Cyberpower. *Georgetown Journal of International Affairs,* 171–179.

Knake, R. K. (2010). *Internet governance in an age of cyber insecurity*. New York: Council on Foreign Relations.

Koley, G. (2017). The Internet is creating Net-States. *International Institute of Information Technology Bangalore*, 1-5.

Krasner, S. (2001). Rethinking the sovereign state model. *Review of International Studies, 27*(5), 17-42. doi:10.1017/S0260210501008014

Kreps, S. (2020). *Social Media and International Relations* (Elements in International Relations). Cambridge: Cambridge University Press. doi:10.1017/9781108920377

Lambach, D. (2020). The territorialization of cyberspace. *International Studies Review, 22*(3), 482–506. doi:10.1093/isr/viz022

Lancelot, J. F. (2020). The deconstruction of nation-state power and the materialization of cyber-states. *Cyberpolitik Journal, 5*(9), 2-21.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7*, 8176-8186. doi:10.1016/j.egyr.2021.08.126

Lin, H. S. (2012). Cyber conflict and national security. *International Politics Enduring Concepts and Contemporary Issues*, 476-489.

Lobell, S. (2017, December 22). Structural Realism/Offensive and Defensive Realism. *Oxford Research Encyclopedia of International Studies*. Retrieved 26 June 2023, from https://oxfordre.com/internationalstudies/view/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-304

Lovink, G., & Riemens, P. (2013). Twelve Theses on WikiLeaks. In: Brevini, B., Hintz, A., McCurdy, P. (eds) *Beyond WikiLeaks*. Palgrave Macmillan, London. doi:10.1057/9781137275745_16

Luiijf, H. A., Besseling, K., Spoelstra, M., & de Graaf, P. (2013). Ten national cyber security strategies: A comparison. *Lecture Notes in Computer Science* (pp. 1–17). Berlin: Critical Information Infrastructure Security.

Marks, J. (2022, March 3). *11 reasons we haven't seen big Russian cyberattacks yet*. Retrieved from The Washington Post: https://www.washingtonpost.com/politics/2022/03/03/11-reasons-we-havent-seen-big-russian-cyberattacks-yet/

Martina, M., & Zengerle, P. (2023, March 9). *FBI chief says TikTok 'screams' of US national security concerns*. Retrieved from Reuters: https://www.reuters.com/technology/fbi-chief-says-tiktok-screams-us-national-security-concerns-2023-03-08/

Maurer, T. (2011). WikiLeaks 2010: A glimpse of the future? *Discussion Paper 2011-10* (pp. 1-49). Cambridge, MA: Belfer Center for Science and International.

Mayersen, I. (2019). *Anonymous took the hacktivism community with them when they died: Is this good or bad?* Retrieved July 18, 2023, from Techspot: https://www.techspot.com/news/80138-anonymous-took-hacktivism-community-them-when-they-died.html

McKinsey. (2022, August 17). *What are Industry 4.0, the Fourth Industrial Revolution, and 4IR?* Retrieved June 11, 2023, from McKinsey & Company: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir#/

Meade, A., Josh, T., & Hurst, D. (2021, February 23). *Facebook reverses Australia news ban after governmrnt make media code amendmests*. Retrieved from The Guardian: https://www.theguardian.com/media/2021/feb/23/facebook-reverses-australia-news-ban-after-government-makes-media-code-amendments

Milmo, D. (2022, February 27). *Anonymous: The hacker collective that has declared cyberwar on Russia*. Retrieved from The Guardian: https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia

Monti, A., & Wacks, R. (2021). *National security in the new world order: Government and the technology of information*. London: Routledge.

Mueller, M. L. (2020). Against sovereignty in cyberspace. *International Studies Review, 22*(4), 779–801. doi:10.1093/isr/viz044

National Academy of Sciences. (2015). *Cybersecurity dilemmas: Technology, policy, and incentives: Summary of discussions at the 2014 Raymond and Beverly Sackler U.S.-U.K. Scientific Forum.* Washington, DC: The National Academies Press. doi:10.17226/21833.

Net Politics. (2020, December 7). *Is global antitrust up to the challenge of Big Tech?* Retrieved June 24, 2023, from Council on Foreign Relations: https://www.cfr.org/blog/global-antitrust-challenge-big-tech

Norton, Q. (2012, January 11). 2011: T*he Year Anonymous Took On Cops, Dictators and Existential Dread*. Retrieved from Wired: https://www.wired.com/2012/01/anonymous-dicators-existential-dread/

Nye, J. S. (2010, May). *Cyber power.* Retrieved from Belfer Center for Science and International Affairs: https://www.belfercenter.org/publication/cyber-power

Nye, J. S. (2022). The end of cyber-anarchy?: How to build a new digital order. *Foreign Affairs, 101*(32), 32-42.

Oremus, W. (2017, November 17). *Big Tobacco. Big Pharma. Big Tech? The rise of a new epithet, and what it means for Silicon Valley*. Retrieved from SLATE: https://slate.com/technology/2017/11/how-silicon-valley-became-big-tech.html

Patel, K., & Chudasama, D. (2021). National security threats in cyberspace. *National Journal of Cyber Security Law, 4*(1), 12-20.

Perritt, H. H. (1998). The Internet as a threat to sovereignty? Thoughts on the Internet's role in strengthening national and global governance. *Indiana Journal of Global Legal Studies, 5*(2), 423-442.

Philpott, D. (1995). Sovereignty: An Introduction and Brief History. *Journal of International Affairs, 48*(2), 353–368.

Pieterse, J. N. (2012). Leaking Superpower: WikiLeaks and the contradictions of democracy. *Third World Quarterly, 33*(10), 1909-1924. doi:10.1080/01436597.2012.728324

Pitrelli, M. (2022, July 28). *Hacktivist group Anonymous is using six top techniques to 'embarras'Russia*. Retrieved from CNBC: https://www.cnbc.com/2022/07/28/how-is-anonymous-attacking-russia-the-top-six-ways-ranked-.html

Ray, M. (2023). *WikiLeaks*. Encyclopedia Britannica. https://www.britannica.com/topic/WikiLeaks

Reardon, R., & Choucri, N. (2012). The role of cyberspace in international relations: A view of the literature. *Proceedings of the 2012 ISA Annual Convention* (pp. 1-34). San Diego, CA: International Studies Association.

Reveron, D. S. (2012). *Cyberspace and national security: Threats, opportunities, and power in a virtual world.* Washington DC: Georgetown University Press.

Rivera, J. (2015). Achieving cyberdeterrence and the ability of small states to hold large states at risk. *7th International Conference on Cyber Conflict: Architectures in Cyberspace* (pp. 7-24). Tallinn: NATO CCD COE Publications. doi:10.1109/CYCON.2015.7158465

Rizvi, K. (2018). *Nation-states to net-states: Power in the hyper-connected age*. Retrieved December 12, 2022, from Observer Research Foundation: https://www.orfonline.org/expert-speak/nation-states-to-net-states-power-in-the-hyper-connected-age/

Rosenstand, C. A., Gertsen, F., & Vesti, H. (2018). A definition and a conceptual framework of digital disruption. *The ISPIM Innovation Summit: Building the Innovation Century* (pp. 1-8). Stockholm: The Name of The Game.

Ross, P., & Maynard, K. (2021). (2021) Towards a 4th industrial revolution,, 13:3, , DOI:. *Intelligent Buildings International, 13*(3), 159-161. doi:10.1080/17508975.2021.1873625

Roussi, A. (2022, September 9). *Meet Killnet, Russia's hacking patriots plaguing Europe* . Retrieved from Politico: https://www.politico.eu/article/meet-killnet-russias-hacking-patriots-pl aguing-europe/

RTVE. (2022, February 26). *Anonymous declara la ciberguerra a Rusia y a Putin por Ucrania*. Retrieved from RTVE: https://www.rtve.es/noticias/20220226/anonymous-declara-ciberguerra-rusia-ucrania/2297941.shtml

San Martin, N. (2022, October 15). *Guacamaya documenta la injerencia de la Sedena y el desdén de la Consejería Jurídica a la CIDH*. Retrieved from Proceso: https://www.proceso.com.mx/reportajes/2022/10/15/guacamaya-documenta-la-injerencia-de-la-sedena-el-desden-de-la-consejeria-juridica-la-cidh-295199.html

Scapolo, F. (2021). *Twitter Permanently Bans Donald Trump. What Does That Mean For Us?* Retrieved July 17, 2023, from Institute for Internet and the Just Society: https://www.internetjustsociety.org/twitter-permanently-bans-donald-trump-what-does-that-mean-for-us

Schmidt, E., & Cohen, J. (2010). The Digital Disruption: Connectivity and the Diffusion of Power. *Foreign Affairs, 89*(6), 75–85.

Schwab, K. (2015, December 12). *The Fourth Industrial Revolution: What it means and how to respond*. Retrieved from Foreign Affairs: https://www.foreignaffairs.com/world/fourth-industrial-revolution

Schwab, K. (2017). *The Fourth Industrial Revolution.* Switzerland: Penguin Books Limited.

Schwab, K. (2023). *The Fourth Industrial Revolution*. Retrieved from Encyclopedia Britannica. https://www.britannica.com/topic/The-Fourth-Industrial-Revolution-2119734

Sepulveda, N. (2022, September 22). *Hackeo masivo al Estado Mayor Conjunto expuso miles de documentos de áreas sensibles de la defensa*. Retrieved from Ciperchile: https://www.ciperchile.cl/2022/09/22/hackeo-masivo-al-estado-mayor-conjunto-expuso-miles-de-documentos-de-areas-sensibles-de-la-defensa/

Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security, 14*(1), 129-136.

Shead, S. (2021, February 19). *It will 'annoy a huge group of the population': How Australians have responded to Facebook's news ban*. Retrieved from CNBC: https://www.cnbc.com/2021/02/19/australians-respond-to-facebooks-news-ban.html

Shen, Y. (2016). Cyber sovereignty and the governance of global cyberspace. *Chinese Political Science Review, 1*, 81–93. doi:10.1007/s41111-016-0002-6

Sheehan, M. (2018). *How Google took on China—and lost*. Retrieved January 20, 2023, from MIT Technology Review:

https://www.technologyreview.com/2018/12/19/138307/how-google-took-on-china-and-lost/

Shull, A., & Hilt, K. (2021). Securing cyberspace in an age of disruption: A glimpse at the rising threatscape. *Canadian International Council, 69*(27), 1-13.

Sifry, M. L. (2011). *WikiLeaks and the age of transparency*. New York: Yale University Press.

Sigholm, J. (2013). Non-State actors in cyberspace operations. *Journal of Military Studies, 4*, 1-37. doi:10.1515/jms-2016-0184.

Singel, R. (2008). *War breaks out between hackers and Scientology -- There can be only one*. Retrieved July 18, 2023, from Wired: https://www.wired.com/2008/01/anonymous-attac/

Singer, P. W. (2001). Corporate Warriors: The Rise of the Privatized Military Industry and Its Ramifications for International Security. *International Security, 26*(3), 186–220.

Sitaraman, G. (2020). Too big to prevail: The national security case for breaking up big tech. *Foreign Affairs, 99*(2), 116-126.

Smith, A. (2018, March 21). *There's an open secret about Cambridge Analytica in the political world: It doesn't have the 'secret sauce' it claims*. Retrieved June 23, 2023, from INSIDER: https://www.businessinsider.com/cambridge-analytica-facebook-scandal-trump-cruz-operatives-2018-3?r=US&IR=T

Sorell, T. (2015). Human Rights and hacktivism: The cases of Wikileaks and Anonymous. *Journal of Human Rights Practice, 7*(3), 391–410. doi:10.1093/jhuman/huv012

Spruyt, H. (2002). The origins, development, and possible decline of the modern state. *Annual review of political science, 5*(1), 127-149. doi: 10.1146/annurev.polisci.5.101501.145837

Steiger, S., Harnisch, S., Zettl, K., & Lohmann, J. (2018). Conceptualising conflicts in cyberspace. *Journal of Cyber Policy, 3*(1), 77-95. doi:10.1080/23738871.2018.1453526

Stevens, T., & Kavanagh, C. (2021). Cyber Power in International Relations . In P. Cornish, *The Oxford Handbook of Cyber Security* (pp. 66–81). Oxford: Oxford Handbooks.

Štitilis, D., Pakutinskas, P., & Malinauskaitė, I. (2017). EU and NATO cybersecurity strategies and national cyber security strategies: A comparative analysis. *Security Journal, 30*, 1151–1168. doi:10.1057/s41284-016-0083-9

Symington, A. (2009, September 1). *Exposed: Wikileaks' secrets*. Retrieved July 19, 2023, from Wired: https://www.wired.co.uk/article/exposed-wikileaks-secrets

The Wall Street Journal. (2021). *The Facebook files: A Wall Street Journal investigation*. Retrieved June 23, 2023, from The Wall Street Journal: https://www.wsj.com/articles/the-facebook-files-11631713039

Thornton, C., & Toh, M. (2021, February 25). *Australia passes new law* *requiring Facebook and Google to pay for news*. Retrieved from CNN Buisness: https://edition.cnn.com/2021/02/24/media/australia-media-legislation-facebook-intl-hnk/index.html

Tidy, J. (2022, March 20). *Anonymous: How hackers are trying to undermine Putin*. Retrieved from BBC: https://www.bbc.co.uk/news/technology-60784526

Tiedke, A. S. (2022). S*elf-statification of corporate actors?: Tracing modes of corporate engagements with public international law*. European University Institute. Retrieved from http://hdl.handle.net/1814/74562

Tonhauser, M., & Ristvej, J. (2019). Disruptive acts in cyberspace, steps to improve cyber resilience at National Level. *Transportation Research Procedia, 40*, 1591-1596. doi:10.1016/j.trpro.2019.07.220.

Uchill, J. (2022, 23 May). *Cyber feud between Anonymous and Killnet groups unlikely to affect others*. Retrieved from SCMedia: https://www.scmagazine.com/analysis/cyber-feud-between-anonymous-and-killnet-groups-unlikely-to-affect-others

Twitter. (2021). *Permanent suspension of @realDonaldTrump*. Retrieved July 17, 2023, from Twitter Blog: https://blog.twitter.com/en_us/topics/company/2020/suspension

Volle, A. (2023, June 17). *Anonymous*. Retrieved from Encyclopedia Britannica: https://www.britannica.com/topic/Anonymous-hacking-group

Walker, K. (2022). *Google at the Copenhagen democracy summit*. Retrieved January 19, 2023, from Google: https://blog.google/outreach-initiatives/public-policy/google-at-the-copenhagen-democracy-summit/

Waltz, K. N. (1979). *Theory of International Politics*. New York: Random House.

Waltz, K. N. (2000). Structural Realism after the Cold War. *International Security, 25*(1), 5–41.

Waltz, K. N. (2003). The anarchic structure of world politics. In R. J. Art, & R. Jervis, *International Politics: Enduring Concepts and Contemporary Issues* (pp. 49-69). London: Pearson.

Wexler, M. N., & Oberlander, J. (2023). The new normal: governance, disruption and the post-truth era. *Transforming Government: People, Process and Policy*, 1-13. doi:10.1108/TG-12-2022-0166

Wichowski, A. (2017). *Net States Rule the World; We Need to Recognize Their Power*. Retrieved December 12, 2022, from Wired: https://www.wired.com/story/net-states-rule-the-world-we-need-to-recognize-their-power/

WikiLeaks. (2015, November 3). *What is WikiLeaks*. Retrieved July 19, 2023, from WikiLeaks: https://wikileaks.org/What-is-WikiLeaks.html

Wong, J. C. (2018, March 22). *Mark Zuckerberg apologises for Facebook's 'mistakes' over Cambridge Analytica*. Retrieved June 23, 2023, from

The Guardian: https://www.theguardian.com/technology/2018/mar/21/mark-zuckerberg-response-facebook-cambridge-analytica

Wriston, W. B. (1997). Bits, bytes, and diplomacy. *Foreign Affairs, 76*(5), 172-174.

Wyler, G. (2012, March 12). *Documents show homeland security was tracking occupy wall street even before the first protest*. Retrieved July 18, 2023, from INSIDER: https://www.businessinsider.com/department-of-homeland-security-tracking-occupy-wall-street-from-beginning-2012-3?r=US&IR=T

Yang, F., & Gu, S. (2021). Industry 4.0, a revolution that requires technology and national strategies. *Complex & Intelligent Systems, 7*, 1311–1325. doi:10.1007/s40747-020-00267-9

Yang, Y., & Goh, B. (2020, August 5). *Timeline: TikTok's journey from global sensation to Trump target*. Retrieved from Reuters: https://www.reuters.com/article/us-usa-tiktok-timeline-idUSKCN2510IU

Yeo, S. (2016). Geopolitics of search: Google versus China? *Media, Culture & Society, 38*(4), 591–605. doi:10.1177/0163443716643014