Updating International Relations for the Information Age

Re-examining the notions of security and sovereignty in the digital age

Beuze, J. (Jasper)
S2163667 mail: j.beuze@umail.leidenuniv.nl

Table of Contents

Introduction

In today's ever globalizing world the spread of and dependence on new information and communication technologies (ICTs) has risen exponentially. With the internet, email, satellite communications and mobile phones permeating everyday life on almost every conceivable level and becoming integral to the functioning of modern society, they have also embedded themselves into our political, economic and social lives. The interconnectedness of individuals in this digital landscape poses some real challenges to the classical role of the state in the current world order. As Henry Kissinger argues in *World Order: "cyberspace challenges all historical experience."* He clarifies this by saying, "*When individuals of ambiguous affiliation are capable of undertaking actions of increasing ambitions and intrusiveness, the definition of state authority may turn ambiguous."* (Kissinger, 2014, pp. 344-345). The physical barriers and borders like mountains, rivers and walls that divided enemies and adversaries during the last century are no longer the strong demarcations of sovereignty and security that they used to be. As has become increasingly visible in the ongoing controversy concerning the Russian involvement in the US elections of 2016 for example. Hackers and trolls are able to act with unprecedented impunity and guile in the digital space, bringing into question what Lucas Kello calls the "moral order of the world" (Kello, 2017); allowing new players to enter the game, with increasingly disruptive consequences to the relevance of the current model of state centered international relations.

The possibilities and problems that the *Information Revolution* has unleashed with regards to notions of security and sovereignty pose a significant challenge to existing theories within the field of international relations (IR) and although some work has been done addressing these issues on a policy level, a clear reconciliation with international relations theory remains absent. Until recently the *modus operandi* within IR has been to ignore the information revolution as revolutionary and try to fit its components into the system of conventional state-craft principles. This lack of theory level study has resulted in a more pragmatic approach towards addressing cyber-security concerns that can produce unintended consequences and instability in the global order. The possibility of undermining this global order is exactly the reason more in-depth analysis of the influence of the information revolution on state security and sovereignty is needed. The information revolution has opened up a new theater of interaction for states, organizations and individuals and has, in a very paradoxical way, made it both harder and easier to track and influence these interactions. The largely ungoverned territory of cyberspace has given states and non-state actors more leeway in influencing the global order as the threat of being found out or getting caught is lower compared to more conventional forms of, for example, military action. Still in its infancy, cyber warfare already poses a paradigm shift for contemporary armed forces. As nations have been slow to adapt to these changes brought forth by the information revolution, a need for more coherent theoretical approaches to cyberspace is warranted. Reconstituting the notion of security and sovereignty in the framework of cyberspace will enable a better understanding of the impact of new technology on the social and political level of international relations, updating it for the post-information revolution era. This I hope to achieve in my paper by answering my main research question:

To what extend has the information revolution affected the notions of security and sovereignty within international relations theory?

To be able to answer this question, the paper will be structured as followed. Firstly, I will give a brief historical overview of the three different stages of the information revolution as they occurred over time and the long-term trends and effects they had on the field of international relations and why they must be considered revolutionary. Secondly, I will be discussing the contested concepts of security and sovereignty in IR theory and the ongoing debate on widening these notions or narrowing them. Thirdly, I shall look into the differing paths that have presented themselves to states in dealing with these core notions of security and sovereignty and argue for a differing role of the state in international relations theory. Concludingly I hope to purpose a different foundational framework for international relations theory that better accounts for the issues posed by the information revolution and is more applicable to the networked world it has helped create.

Information Revolution background

As with the industrial revolution, the point of origin for the information revolution remains contested. One might trace its lineage back over five hundred years to the invention of the Gutenberg printing press, or maybe even further to the origin of human civilization and the invention of writing (Rayward, 2014; Owen, 2015). What characterizes all these proposed revolutions however, is the emergence of complex, interlinked institutionalized information and communications infrastructures that were both a response to and provided support for the development of and restructuring of human society along political, economic, social and cultural boundaries (Kello, 2017; Aronson & Cowhey, 2010). This paper will limit itself to the most recent iteration of this revolution, following the invention and development of the internet and the ICT revolution this enabled. This chapter will mainly be a technical historic overview of the developments that occurred, as the implications of said developments will be talked about at length in the following chapters. To be able to talk about and understand these implications, some knowledge about the technologies that cause these implications is required. Therefore, this chapter is divided into three subsections; the first addresses the long underlying trends that are at the core of the internet's infrastructure, the second will dive into the commercialization and wider adoption of the internet, and the last section will talk about the current state of internet adoption. The different stages should not be seen as freestanding developments, but more as incremental improvements building upon each other.

Stage 1 the origins of the digital infrastructure

The continued growth and capabilities of the internet is predicated on three main trends that were established from its conception in 1962, when the idea for a global computer network was first envisioned by computer scientist J.C.R. Licklider (Leiner, et al., 1997). The resulting infrastructure that resulted from these trends is the foundation of the internet and drives its further development. These trends also underpin many of the perceived problems and implications that we derive from this new encroaching digital frontier that our society has become increasingly reliant on. Aronson and Cowhey specify these three long-term trends that revolutionized ICT infrastructure as follows (Aronson & Cowhey, 2010):

The first trend revolves around the end points on ICT networks. Starting with connecting individual computers into a network architecture when ARPANET[1] was still under development at the US Department of Defense. Soon other networks were made between universities and other government agencies and eventually these separate networks were incorporated into the system, creating a network of networks and opening the doors for the conception of the internet. Instead of end to end connections, the network started to use nodes or hubs to connect whole networks to each other to cope with the growing size and demands that were placed on the system. Moving away from dumb terminals that were limited in their input and output capabilities, the introduction of

[1] The Advanced Research Projects Agency Network (ARPANET) was an early packet switching network and the foundational structure for the internet. During its lifetime it was expanded upon and conjoined with other networks like the Computer Science Network (CSNET), before it was decommissioned in 1990.

powerful networked personal computer terminals proliferated, and the network became increasingly ubiquitous and heterogeneous. This decentralization in the network architecture made the network more resilient whilst also being one of the main differentiating aspects concerning older ICTs like radio, television and newspapers.[2] The internet can not only accommodate one-to-one, one-to-many or many-to-one communication, it is also able to facilitate many-to-many communications with dazzling speeds and less intermediaries than older forms of communication (Nye, Power in the Global Information Age, 2004).

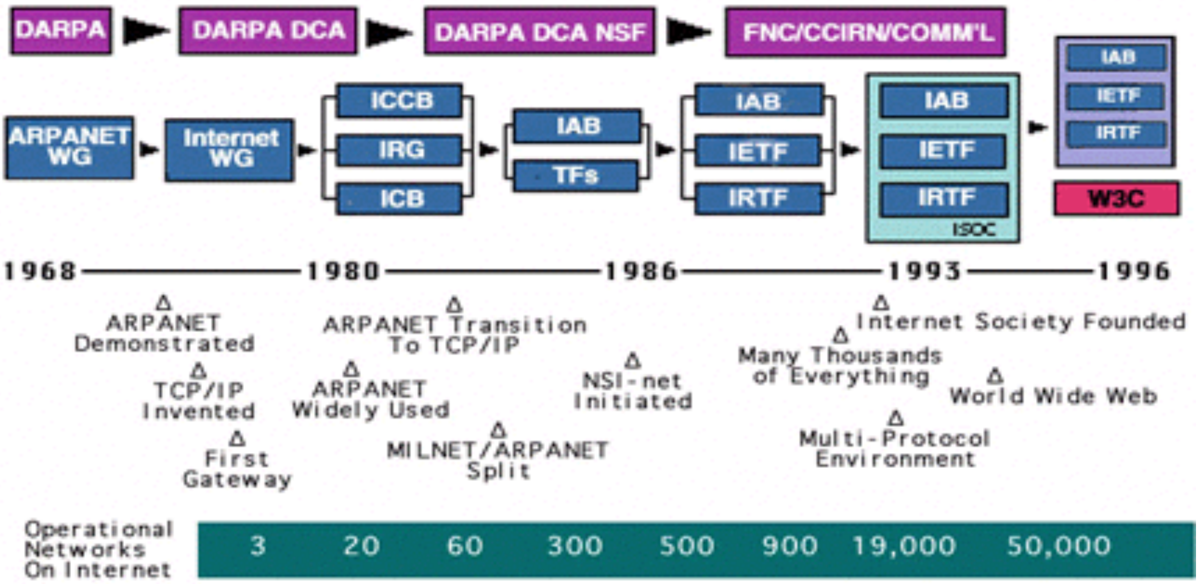

Figure 1 Timeline of the Internet https://www.internetsociety.org/internet/history-internet/brief-history-internet/

The second trend that enabled this explosive growth in network integration and processing power was the price point of speed and quality of service in the ICT markets with Moore's Law being the prime example of this increase in processing power. Moore's Law states that the number of transistors in a dense integrated circuit doubles every two years, effectively meaning an exponential growth in processing power (Moore, 1998).The increasing decentralized nature of the network architecture allowed for faster connection speeds and lower implementation costs. This decrease in cost and increased processing power meant computers became smaller and more suitable for a wide array of tasks, which further increased adoption rates in the developed world. With the move to mobile devices, this increase in adoption has become even more visible with developing countries for instance foregoing old desktop computing and connecting more and more through affordable smartphones and tablets (McCabe, 2013; Aronson & Cowhey, 2010). These developments have helped to bridge the 'digital gap' that divides the haves and have-nots

[2] Making use of packet-switching, data is broken down into small *packets* that can be send through the network individually and along different routes, they are then reassembled at the end point. This ensures that even if one or even most connections within the network would fail, the data can still be transmitted, making it very flexible and resilient. (Singer & Friedman, 2014)

when it comes to access and usage of the new digital medium (Choucri, 2000; Eriksson & Giacomello, 2006).

Thirdly, as the number of nodes and end points on the network has been increasing, so has its sensory and data collection capability. With increases in processing power and continued expansion of the network, the amount and kinds of data that can be collected increases exponentially. Data is no longer restricted to text-based commands on dumb terminals, but end nodes can now record voice and sound (e.g. smartphones), collect pictures, videos, temperature readings and all kinds of other forms of information. With this expansion of the networks capabilities and uses, the benefits of integrating one's own network to acquire access to these capabilities and this information becomes apparent.

It is these main trends that have made the internet possible and continue to drive advancement in the digital sphere and would ultimately result in opening up the internet for commercial use.

Stage 2 the widening web of commercialization

During the 1980s, commercial interest in the internet started to increase, as the possible uses of the technology became increasingly apparent and developments in computer design made personal computing accessible to the public. When the Internet Activities Board (IAB) held a three-day conference for commercial vendors that openly showcased the inner workings of the ARPANET architecture and internet protocol (TCP/IP) that governs communications on the network, the stage was set for the internet to go public. Frequent cooperation and discussion between the commercial and scientific communities about the possible development and structure of the internet's infrastructure resulted in quick commercial adoption of the new technology (Leiner, et al., 1997). With the production of the first commercial router, companies were able to connect the in-house networks to the internet ushering in a new generation of computer networking architecture that was more decentralized, ubiquitous and heterogeneous.

Another main contributor to the fast adoption of internet during the late 80s and the 90s in the American commercial sector was the breakup of AT&T in 1984. By breaking up the telecommunications monopoly AT&T enjoyed in North-America, the telecommunications market was opened for competition between new providers (Aronson & Cowhey, 2010). With the internet being the hot new technology, competition over connection speeds and services boosted the necessary investments needed to build the real-world physical infrastructure required for the internet. Coupled with the continuation of Moore's Law, the introduction of the desktop computer and the decreasing cost of these new technologies, internet in the 90s was set to enter not just the offices, but also the individual homes of people.

Alongside the development of the then still wired internet, the second generation (2G) mobile wireless networks experienced explosive growth. Offering increased capacity and quality whilst reducing adoption costs when compared to wired connections, causing in particular developing countries to forego wired connections altogether and focus on wireless telecommunications. Whilst this reduced initial costs for telecommunications it meant the necessary wired infrastructure required for internet was lacking. It would take some time before the large data transmissions characteristic of the internet would go wireless with the wide adoption of Wi-Fi networks in the early 2000s.

As the commercialization of the internet continued, companies that provided internet-based services exploded onto the market. Starting with commercial email service providers and eventually culminating in Netscape going public and starting the 'dot com' boom[3], by the 2000 the market had fully embraced the internet. The invention of the World Wide Web and its underlying HTML programming language resulted in a more user-friendly environment for the average person, giving easier access to all the ongoing data communications and making the information in the internet generally more intelligible. A downside to this development was the fact that consumers and countries had to rely on proprietary software in the form of web browsers to access the internet.

Stage 3 The '*Cheap Revolution'* of web 2.0

The reconfiguration of the web with the introduction of the web 2.0, or more recently called the internet of things, after the initial 'dot com' boom changed the internet architecture even more. A shift towards Grid and Cloud computing means an even more decentralized architecture, where the hardware is no longer built into one big machine or computer, but is shared across different devices, machines and terminals. This decentralized notion is illustrated in Ian Fosters definition of Grid computing (Stockinger, 2007, p. 4):

(1) *coordinating resources that are not subject to centralized control …*
(2) *… using standard, open, general-purpose protocols and interfaces …*
(3) *… to deliver nontrivial qualities of service*

All the while terminals have become cheaper and more powerful. Coined the 'Cheap Revolution' by Rich Kaarlgard (2003), he identifies four trends; The first is the previously mentioned price-performance dynamic and the decreasing costs of data storage. With the introduction of the smartphone, the capabilities of the terminal had changed dramatically. No longer bound to the desktop, access to the internet is now more portable than ever. Secondly, innovations in fiber optics and wireless bandwidth have made faster connections possible over hybrid networks that are no longer solely dependent on wired connections. With this new explosion of the mobile, the hardware connected to the internet is diversifying and modular software support is becoming necessary. The third trend is OS agnostic applications[4] becoming the industry norm, to deal with the increased heterogeneity and ubiquity of computer hardware. And lastly, the way media is distributed on the internet has had far reaching consequences for commerce, journalism and international politics (Aronson & Cowhey, 2010). With the development of OS agnostic software, digital content can be widely converted across networks and terminal systems. Making digital content distribution far easier than conventional media distribution. Essentially challenging the geographic boundaries of traditional broadcast models (Aronson & Cowhey, 2010, p. 5).

[3] The 'dot com' boom or often referred to as the 'dot com' bubble, saw massive speculation of publicly traded tech companies with explosive growth, but eventually leading to a major financial crash of the industry between 2000 and 2002.

[4] OS agnostic stands for operating system agnostic.

The foundation of the internet architecture influences not only its own development as shown in this chapter, but also has profound implications on the way IR theory approaches this new technology. Before elaborating further on the implications this new technology has on the notion of security and sovereignty, we will first have to look at the ongoing theoretical debate on these concepts within the field of IR theory.

Contested Concepts

The choice of addressing the notions of security and sovereignty in this paper is not an arbitrary one. The digital age has problematized the relation between these concepts in novel ways. The absence of clear territorial demarcations in cyberspace for instance, has forced a reconceptualization of the traditional underlying principles of sovereignty and security. This resulting sovereignty gap is explained as follows by Lucas Kello (2017, p. 254): *'The functions of national security provisions and international crisis control no longer belong to the state alone or in some areas even primarily.'* This chapter will address the changing debates around both these concepts. Firstly, by discussing the 'wide' versus 'narrow' debate on security (Buzan, Weaver, & de Wilde, 1998; Eriksson & Giacomello, 2006; Goldman, 2003; Harknett R. , 2003; Arquilla, Thinking about new security paradigms , 2003). Secondly, by addressing the different definitions of sovereignty, and the problems that arise from this and how this relates to the sovereignty gap in cyber space (Addis, 2004; Clunan & Trinkunas, 2008; Lotrionte, 2012; Kello, 2017; Krasner S. D., 1999; Krasner S. D., 2009; Owen, 2015).

Security

Theory level research on the effects of the information revolution on security has been sparse. Whilst some policy analyses have been done with regards to the security of firms and markets, extensive research on the security of states and society has only very recently come to the fore. The specialized literature that has been produced, is almost strictly policy oriented and has an alarmist tendency. (Eriksson & Giacomello, 2006). The main explanation for this lack of interest in the wider security implications of the information revolution can be found in the larger security debate within international relations theory. The entrenched dualism in IR theory with regards to the issue of security, makes it hard for theory and policy concerning cyber security to inform one another and fully integrate the information revolution into IR theory.

But what constitutes security? As defined by Ole Waever:

> "[…] security is a kind of stabilization of conflictual or threatening relations, often through emergency mobilization of the State. Although security in international relations may generally be better than insecurity (threats against which no adequate countermeasures are available), a secure relationship still contains serious conflicts – albeit ones against which some countermeasures have been taken." (Buzan, Weaver, & de Wilde, 1998, p. 4)

It is the use of these emergency measures, or in other words, the use of executive action to tackle issues that differentiates security problems from other issues in the publicly debated political sphere. No longer bound by the rules that dictate the actions within the political sphere, the state for example has greater leeway to deal with the perceived existential threat. Expanding the notion of security to encompass issues that are outside the traditional realms of the military, or issues that deal with the threat or use of force, understandably raises concerns as to overextending the ability to use the drastic emergency countermeasures and trivializing the notion of security.

The process of securitization, as developed by the Copenhagen School, therefore lies at the core of the security debate. Securitization should be understood as a process through which an issue is staged as an existential threat to a referent object which allows for extreme or emergency actions to be undertaken to combat said threat. Securitization primarily consists of a speech act, through which a potential threat is framed as existential and is then successfully lifted from the political sphere into the security sphere. A security problem therefor takes precedence over other problems, because it is argued that not tackling the security problem will make all other problems irrelevant. An important distinction here is that securitization is a speech act, so the security problem does not actually have to be existential, only be portrayed as such. A securitization move is thus only successful when the audience accepts it as being an existential threat worthy of moving into the security sphere. In summary, a successful securitization move has a rhetorical structure consisting of three components: the framing of an existential threat, stating the need for emergency measures to tackle this threat, and breaking free of ordinary rules and oversight to combat the threat. If all these components are successfully argued and find acceptance with the audience, the legitimization of the securitization move is completed and the securitization of the issue is successful (Buzan, Weaver, & de Wilde, 1998).

The current security debate revolves around the two competing stances on securitization. Where one side prefers to keep a narrow definition of issues that can be moved from the public political sphere into the more executive security sphere, mainly military conflict and issues dealing with the use of force. Another side has risen up after the Cold War advocating for expanding security into other areas like the economic, environmental and identity sectors. Concerning the information revolution, both sides seem to have difficulty in dealing with the issues posed by cyberspace.

Traditionalists

The traditionalist perspective on security stems from the (neo)realist school of IR theory that dominated the Cold War and is mainly concerned with the active use of force or the direct threat of force in an anarchic international system of states. Building upon the classical work of writers like Hobbes, Machiavelli, and Rousseau, the realist notion of security experienced a revival in the 20th century due to the work of scholars like E.H. Carr, Hans Morgenthau and Kenneth Waltz. Waltz in particular was very influential in creating the school of neorealism with his seminal work on *Theory of International Politics*. Waltz's starting axiom is the perpetual anarchic state of international affairs that drives the actions of states. Opposed to domestic affairs where the state acts as the central enforcer, there is no higher authority in the international system that can effectively arbitrate conflict, states therefore have to rely solely on themselves to ensure their survival (Waltz, 1979). Waltz's theory was a jumping off point for others like Stephen Walt who expanded upon the balance of power theory, and John Mearsheimer who worked on and was a great advocator of the concept of nuclear deterrence (Mearsheimer, 1983; Walt, 1985).

As is the case with the current information revolution, the traditionalist security paradigm was born out of a necessity to incorporate new technology into security theory, namely the introduction of nuclear weapons technology. Weapons of mass destruction in this realist perspective were viewed as absolute security guarantors. All throughout the Cold War the security strategies were updated when new technology became available, going from the massive number of retaliatory nuclear strikes under Mutually Assured Destruction (MAD) to more tactical intercontinental ballistic nuclear capabilities allowing for local conflicts to be fought (Kello, 2017). Adapting to the incremental developments in technological capabilities, nuclear deterrence served as the strategic cornerstone of the Cold War international system (Goldman, 2003). The bipolar nature of the conflict essentially simplified this strategy, as security posturing only had to be communicated to one clear recipient (Waltz, 1979; Walt, 1985). As Richard Harknett noted in his article on *integrated security*: '*The evolution of this strategy of nuclear deterrence created a unique security system in which the actual continued existence of one's adversary became the basis of one's own security.'* (Harknett R. , 2003, p. 16). Harknett effectively argues that this model of deterrence was a departure from the classical balancing within the offence-defense model, that rested upon the ability to physically take and control territory. This change in security paradigms was not only facilitated by the technological advancements in nuclear capabilities, but also on a systemic level by shifting from a multipolar to a bipolar conceptualization. Following the end of the Cold-War we see similar developments, with advancements in information technologies changing the underlying technological capabilities of actors and a restructuring of the international system to a unipolar or even multidimensional model wherein the primacy of state actors is being questioned. Traditionalist security models fail to recognize or acknowledge this revolutionary nature of the information revolution.

Following the end of the Cold War the traditionalist notions of security found themselves extremely vulnerable, as their theories were unable to predict[5] or explain what happened. The old axioms of deterrence and containment were no longer applicable in a non-bipolar world. Reaffirming their stance on the primacy of the state and the focus on military security, calls for a wider conception of security were largely ignored by traditionalists (Buzan, Weaver, & de Wilde, 1998). Whilst it can be argued that both the nuclear and information revolution are at their core technologically driven revolutions in state capabilities and, therefore, the same security models are applicable to both, the logic is problematic. This is because the information revolution distinguishes itself from the nuclear revolution due to its wider and more complex impact on society (Owen, 2015). Where the destructive power of nuclear weapons fit nicely in the Clausewitzian industrial model of destructive war based on lethality, the information-era model of war is centered on disruption, paralysis and non-lethality (Goldman, 2003). Dubbed *weapons of mass disruption* by Kello, information has become a weapon in the purest sense. No longer just a source of power and intelligence informing military action, information has become force itself (Kello, 2017; Owen, 2015).

Harknett and Kello point to several problems within the traditionalist security model's ability to explain the information revolution, which effectively boils down to three distinct breaks. Firstly, it breaks with the classical security paradigm of effective territorial control. Where traditionally the enemy's presence in domestic territory heralded the failure

[5] Waltz himself acknowledged the predictive shortcomings in *Theory of International Politics*, suggesting that explanation rather than prediction is expected from a good social sciences theory. Stating that unlike the natural sciences, the social sciences cannot run controlled experiments to the same extend to acquire those predictive properties (Waltz, 1979, p. 6).

of security policy, in the cyber sphere it is a starting axiom. Secondly, the complexity of information technology makes it difficult to predict its effects. As integrated network systems constitute the underlying architecture of the internet and the information revolution as a whole, the direct effects of a cyber-attack are difficult to predict, let alone the indirect effects of such an attack. A cyber-attack could therefore result in cascading effects that affect essential activities across a range of sectors and jurisdictions, due to the interconnectedness of systems and the current reliance of society on these complex computer systems for day to day usage. Thirdly, the sheer speed of development in the information and communication sector makes it difficult for strategists to identify, comprehend and master a technology whose technical features change so rapidly (Kello, 2017; Harknett R. , 2003).

Where the narrow conception of security through the traditionalist model runs into problems in cyberspace however is in their concern with the primacy of the state (Kello, 2017; Arquilla, Thinking about new security paradigms , 2003). Where the development of nuclear weapons required substantial investment and large industrial capacity, resources that are almost exclusively available to states, information warfare in contrast requires substantially less resources, making it accessible to a wider range of actors. Actors that fall outside of the traditional international state centric model of international relations. These non-state actors include terrorist groups, corporations, activist groups, online communities, individuals, etc. If we build upon Arquilla's arguments in his work *National Security in the Information Age* and incorporate Kello's and Goldman's arguments, the entry of these new actors in the security framework regarding deterrence poses several problems: that of commensurability, rationality and attribution.

Starting with commensurability, the deterrence models core principle of retaliation in kind, also known as MAD. In this security paradigm, the destructive impact of an attack would match the losses incurred from the immediate counter attack, thereby equalizing the balance of power. But as Kello notes, what if the weapon used is not destructive, but disruptive in its impact? And as Goldman keenly notes; if the only casualty in war is a loss of information, is an immediate counterattack of comparable power the adequate response? And what should be targeted, is physical destruction a proper answer to digital disruption? As mentioned before, the difficulty in predicting the cumulative effects of a cyberattack on integrated networks of complex computer systems, might only escalate further conflict. The discrepancy in assets might also problematize the deterrence strategy of retaliation in kind, as the aggressor might be a small group of insurgents with limited physical means disrupting the infrastructure assets of an entire state (Goldman, 2003; Kello, 2017).

This brings us to rationality. The traditional deterrence security paradigm is heavily influenced by the trinitarian notion of Clausewitzian warfare (Mingus, 2013). According to Clausewitz theory, warfare consists of three components: violent emotion, chance, and rational calculation (Clausewitz, 1940). It is the rational calculation of states within the anarchic state model underlying the security paradigm that traditionalists take for granted. Traditionalists often reduce the security problems of international anarchy to a theory in which a state's material gains take precedent over other issues like ideology for example. To combat the inherent uncertainty of the anarchic system, the rational option for states would be to try to expand their material capabilities. This notion does not necessarily result in peace and harmony however, as underlying anxieties within state rivalries remain unresolved. A state might only feel a limited sense of security when a parity or excess in material assets is achieved comparable to its rival. In other words, when a balance of power is established. This would be rational, but under extreme ideological conviction for example, a state might decide that conflict is necessary or preferable (Kello, 2017). The example of Nazi Germany comes to mind, where the ideological conviction of the Nazi's made conflict inevitable. Non-state actors that fall outside this traditional security paradigm can be even more erratic in their actions. A group of dissidents is not weighed down by the responsibilities attributed to states and could operate outside their rational framework, thereby subverting the political order within the states system (Eriksson & Giacomello, 2006; Kello, 2017; Goldman, 2003; Arquilla & Ronsfeldt, Networks and Netwars: The future of terror, crime and militancy, 2001). Therefore, the same rationality that is used by states is incongruent with the rationality that might be used by non-state actors as they don't inhabit the same level of analysis scheme within the theory of traditional security paradigms. More clarification on the levels of analysis approach in international relations theory is in the next section on sovereignty, for now it suffices to understand that the state level of analysis does not necessarily have to be the primary level of analysis. Or as stated by Buzan, Weaver, and de Wilde in their work *Security: A New Framework for Analysis*:

> "If one wants to see political time and space structured along different lines, the levels of analysis scheme in its neorealist form will be seen as problematic. There is no necessity for levels to privilege states – the unit level can encompass much more than states." (Buzan, Weaver, & de Wilde, 1998, p. 7)

Therefore, the study of security problems resulting from the information revolution cannot be solely based on the basis of rational interstate dealings (Kello, 2017).

Finally, we have the problem of attribution. The potential for anonymity in the digital sphere combined with the possible use of proxies, severely complicates the strategy of deterrence. As deterrence requires a quick situational awareness of the scope of an attack and the location of the source of this attack to be effective, the inability to quickly attribute an attack reduces the effectiveness of deterrence strategies (Harknett R. , 2003). For one, assessing the scope of an attack in the digital sphere is problematic, as infiltrating a system to spy and retrieve data could also be the first step in a larger assault on a system. Unfortunately, there is no quick way of ascertaining this beforehand. Also, the sheer speed of digital interactions means that any reaction to an ongoing attack is usually already too late. Judging the intent behind system infiltrations, and the proper response, is almost impossible if the attacker cannot be quickly identified. Whilst the use of proxies is not anything new and was used extensively during the Cold War, the operating costs of maintaining such proxies in the digital sphere is substantially lowered, increasing the number of proxies available to any one actor. This also means that the hiring of proxies, for example lone hacker groups, is no longer the sole prerogative of states, but companies might start employing these groups too in doing so further broadening the number of involved actors in the security sphere. It should be self-evident that an increase in actors makes attributing actions to one specific actor more difficult. The difficulty in this multidimensional conflict, as Harknett notes, is that the signaling necessary for deterrence security posturing is open to greater misinterpretation either because the threat is made too imprecisely or because it is directed too narrowly (Harknett R. , 2003).

In summary, traditionalists fail to recognize the revolutionary aspect of the information revolution and try to assimilate these new threats into conventional theories. Where the strategy of deterrence was applicable to the problems posed by nuclear weapons, the current conservative tendencies of the traditionalist side within security studies is unable or unwilling to deal with the paradigmatic shift that the information revolution and use of virtual weapons requires. The core security principle in international order no longer concerns the balance of power, but as Kello notes, the balance of players. The state is no longer the sole and primary actor in the security framework. Furthermore, the binary conception of conflict during the Cold-War no longer applies in the current multidimensional order. Conflict itself no longer consist of a clear delineation between war and peace but has become opaquer in its operations (Arquilla, Thinking about new security paradigms , 2003). Kello notes that: *'A new form of mid-spectrum harm and international rivalry that is neither fatal or physically destructive like traditional war, nor desirable or even tolerable like conventional forms of peaceful rivalry.'* has emerged, labeling it as *unpeace* (Kello, 2017, p. 249). The adherence to meta-level theoretical rationalism in the traditionalist camp has failed to account for the paradigmatic shifts resulting from the end of the Cold War and the information revolution and has left a considerable gap for the wideners to advocate for a reconceptualization of the international security framework.

Wideners

As stated above, the call for a wider conception of security studies came out of a dissatisfaction with the traditional narrow notions of security issues as they were unable to cover the issues that presented themselves after the Cold War. The breakup of the traditional bipolar dynamic and introduction of non-state actors in international affairs has frayed the notion of deterrence. The cracks in the traditional security paradigm already appeared during the closing years of the Cold War, when economic and environmental issues were raised into the security sphere by wideners. This issue-driven widening was expanded upon after the fall of the Berlin Wall by new concerns about identity and transnational crime. But, 'expanding the security agenda is not a simple or a trivial act, nor is it without political consequences.' (Buzan, Weaver, & de Wilde, 1998, p. 195).

The main criticism regarding the widening of the notion of security comes from risking its intellectual coherence by overextending the security agenda. Widening the security agenda enlarges the knowledge and understanding necessary to comprehend security studies and individual security issues. Furthermore, it broadens the call for wider state mobilization on these issues that are now brought into the security sphere, putting more strain and pressure on governmental institutions to act accordingly. Whilst simultaneously elevating the word 'security' into a universally good thing, or a direction towards which all relations should move. For example, the propensity of liberal economic security issues to spill over into other areas is a slippery slope concerning securitization. This critique of the widener stance on the notion of security is valid and as Buzan, Weaver and Wilde noted, should be guarded against.

The call for widening the notion of security started with the increase of liberalist thought and policy and the rise of liberal democracy in international affairs during the latter half of the twentieth century. Originating from Kant's democratic peace theory, liberalism surged after the Second World War and was revised for the post-war world by Robert O.

Keohane and Joseph S. Nye in their seminal work *Transnational Relations and World* Politics, which linked democratic peace with the economic ties of capitalism (Keohane & Nye, Transnational relations in World Politics , 1971; Keohane R. O., After Hegenomy: Cooperation and Discord in the World Political Economy, 1984). Another notable widener and constructivist is Alexander Wendt who criticized Waltz's anarchic model in his work *Social Theory of International Politics* (Wendt, 1999). Consisting of a mix of liberal and critical theorists, the wideners contest the traditionalist approach on two key areas. Firstly, they propose that the narrow view on security should be broadened to encompass the 'new' threats and challenges that face the globalized and post-Cold-War world. Issues not confined solely to the military sector, but also the political, societal, economic, and environmental sectors. The main contributor to this broader sectoral approach has been the Copenhagen School, of which Buzan, Weaver and Wilde are the most prominent theorists. Whilst it didn't yet address the notion of cybersecurity, their work on *Security: A New Framework for Analysis* will be discussed later in this chapter, as it is one of the more prominent and useful theories to have arisen out of the widener camp. Secondly, the wideners have advocated for a range of 'new' actors in analyzing security concerns. Ranging from NGOs, social movements, terrorist groups, criminal cartels, private companies, to individuals (Eriksson & Giacomello, 2006). However, like their traditionalist counterparts, the wideners have yet to address the issue of cybersecurity in extensive detail.

Whilst most liberals tend to refute the realist notions on security that are most prevalent in the traditionalist's framework, they tend to share the same underlying rationalistic and epistemological approach. The shared emphasis on interest-based interaction and utilitarian roots within liberalism and rationalism for example distinguishes them from the more constructivist approaches (Keohane & Nye, 1987). The distinguishing factor between realists and liberalists however, boils down to their competing world views. Where realists tend to be more pessimistic in their assertion of global affairs, highlighting the anarchic system and its preference for explaining interactions between states in terms of self-interest and survival. Liberalists have a more optimistic view, highlighting economic ties and interactions and cooperation between states through international institutions to try and resolve conflicts peacefully. The biggest contribution of the liberalists has been the emphasis on the plurality of world actors with regards to the development of security theory (Eriksson & Giacomello, 2006). Highlighting not only the importance of international institutions and organizations but also private companies, activist groups, criminal cartels and other non-state actors. Another contribution has been the development of complex interdependence theory by Joseph Nye and Robert Keohane that together with Nye's notion of *soft power* have been very influential in developing a neoliberalist notion of international relations theory (Keohane & Nye, Power and Interdependence in the Information Age, 1998).

Where the realist perspective on power dealt mainly with coercion or *hard power*, Joseph Nye introduced the concept of cooption in his coining of the term *soft power*.

> "When one country gets other countries to want what it wants-might be called co-optive or soft power in contrast with the hard or command power of ordering others to do what it wants." (Nye, 1990, p. 166)

With his introduction of *soft power*, Nye puts more emphasis on economic and social factors within international relations. A deviation from the mainly military-security concerns of the realists (Keohane & Nye, 1987). With their development of complex interdependence theory, Keohane & Nye tried to bridge the gap between realist and liberal conceptions of power, highlighting the relation between interdependence and potential power resources picturing them as '*[…] two sides of a single coin*' (Keohane & Nye, 1987, p. 730). Whilst Nye does stress the importance of *soft power* in the digital age, with its increase in global communication channels that easily transcend sovereign boundaries, he does not extensively elaborate on, or incorporate digital security issues within his theoretical framework. Ericksson and Giacomello have noted that implicitly two socioeconomic trends can be extrapolated from this liberal theory: (1) the expanding partnership between the public and private sectors to provide services and (2) the merging of the civil and military spheres. These trends have blurred the lines between different segments of societies that pertain to distinctions in jurisdiction, competencies, duties and risks (Eriksson & Giacomello, 2006). Resulting in a plurality of actors within international relations outside of the purely state-centric view of realist theory.

Contrary to the liberalists, the constructivists within the widener camp refute the meta-theoretical rationalism inherent to both realism and liberalism. Where both liberal and realist theories have had trouble adjusting to the paradigmatic shifts resulting from the end of the Cold War, constructivists jumped on the chance to bridge the gap between the traditional realist and contemporary postmodern theories within the field of international relation theory. Distinguishing between a material reality and a social reality, that is socially constructed and therefore susceptible to change, constructivists are interested in the creation and workings of this social reality. Consisting of a broad range of disciplines, methodologies and theories, constructivism is less restricting on what can be perceived as a security threat, which is both its main strength and weakness (Eriksson & Giacomello, 2006).

In *Security: A New Framework for Analysis* Buzan, Weaver and de Wilde hailing from the Copenhagen School argue for an approach that tries to constrain this ever expansionist tendencies of the widener constructivist agenda and somewhat bridge the gap with traditionalist nations on security. In their words:

> "Pursuing the wider security agenda requires giving careful thought to what is meant by security and applying that understanding to a range of dynamics, some of which are fundamentally different from military-political ones." (Buzan, Weaver, & de Wilde, 1998, p. 195)

Their previously discussed process of securitization has proven to be a useful tool in assessing and explaining which issues should be raised from the political sphere into the security sphere. Whilst their sectoral approach fails to fully incorporate the information revolution and the level of analyses within their sectoral approach still strongly favors the state as the prime harbinger of security within international relations, it does offer a better framework for security analysis in the digital sphere than the traditionalist approach.

In summary, the entrenched dualism within international relations theory prevents theory and policy on cyber security issues from effectively informing one another. The traditionalist mentality of old wine in new bottles when it comes to the new security issues brought forth by the information revolution, and their reluctance to adjust to this paradigmatic shift, means that theory is increasingly decoupled from practice. As discussed, the old traditionalist model of deterrence is no longer applicable in the increasingly multidimensional digital world. Wideners have tried to broaden the notion of security to account for this multidimensionality by issue-driven expansion of the notion of security. Whilst the expansion of security to cover economic, environmental, societal and political issues have been illuminating for international relations theory, wideners have yet to address the digital sphere with a coherent in-depth analysis. Still, some of the wideners work is helpful in addressing the security concerns of the digital sphere. The development of the model for securitization by the Copenhagen School effectively explains the way in which issues get securitized and is also applicable in the digital sphere. The inclusion of non-state actors within the international system by liberalists opens up international relations theory to the increasing capabilities of corporations, activist groups, NGO's, terrorist groups and individuals amongst others, made possible in large part by the information revolution. Also, the non-rationalist approach by constructivists might go a long way in explaining the behavior of these new actors within the international system. All in all, the digital sphere has yet to receive the theoretical analysis that it needs to be fully understood and incorporated into international relations theory.

Sovereignty

As was apparent in the section on security, the primacy of the state within international relations theories is one of the core underlying disputes across the field of the contemporary international relations debate. State sovereignty has arguably been one of the guiding principles of international relations since the Peace of Westphalia and, in the eyes of many, it is increasingly being challenged by the process of globalization, of which the information revolution is a large constituting factor (Addis, 2004). However, as will be discussed in this section, the notion of state sovereignty has been problematic from its inception and reevaluating the relevance of this core principle in international relations theory might help in bettering our understanding of its function within the digital sphere.

As we have seen in the previous section, the information revolution has caused significant paradigmatic shifts in the underlying principles of traditional notions of security. New actors, new technological developments and a resistance to adapt pre-existing theories have made it difficult to effectively address the concerns posed by the digital era. The entrenched dualism within the field of international relations is not only apparent within security studies but can also be found within the debate on state sovereignty. Where one side sees territorial sovereignty as an impediment to the technological progress of the information revolution and purposes the nation-state to be on its last legs, another group defends the resilience and usefulness of the territorial state within the framework of international relations. To fully understand the differing views between these two camps, we shall have to untangle the differing notions of sovereignty that are often conflated within the wider debate.

Organized Hypocrisy

The term sovereignty has been used in differing ways, complicating any debate regarding its core principles and definition. To untangle this convoluted definition of sovereignty Stephen Krasner has made a useful distinction between four different types of sovereignty (Krasner S. D., 1999). Whilst these four variants are not logically coupled or covariate in practice, they do highlight the fundamental distinctions between authority and control that are embedded within the different usages of the term sovereignty. The four usages are: (1) domestic sovereignty, (2) interdependence sovereignty, (3) international legal sovereignty, and (4) Westphalian sovereignty. To understand the differences between these usages, we need to understand the difference between authority and control. As Krasner puts it:

> "Authority involves a mutually recognized right for an actor to engage in specific kinds of activities. If authority is effective, force or compulsion would never have to be exercised. Authority would be coterminous with control." (Krasner S. D., 1999, p. 10)

Control, on the other hand, can also lead to systems of authority over time. If an enforced rule or policy is instrumentally effective in controlling behavior, for example, people might come to consider it as normatively binding (Sugden, 1989). So, whilst control can be achieved through force alone, authority requires mutual acceptance of certain rules or norms and therefore cannot be imposed by force itself. The behavior of actors in the political or social spheres are therefore informed by logics of consequence, in which control is the key issue, or logics of appropriateness, in which authority is the main factor. It is especially in the realm of authority that the concept of sovereignty becomes problematic, in large part because of its socially constructed nature.

So how do the distinctions between control and authority relate to the four usages of sovereignty? Well firstly, the line between control and authority can be hazy at times, as domestic sovereignty exemplifies. Domestic sovereignty entails the organization and effectiveness of political authority and institutional control within a state. What is the recognized authority structure within a state, and how effective is it a maintaining their level of control within the state? Interdependence sovereignty deals exclusively with control, more precisely the effective control of territorial boundaries and who or what might cross them. When reading about sovereignty loss, this is most often referred to when talking about the effects of globalization. However, this does not necessarily mean domestic sovereignty is affected, or Westphalian sovereignty for that matter. A state might not be in total control of its trans-border flows but still retain effective authority or control over its territory. Loss of interdependence sovereignty has typically involved international legal sovereignty, as nations have entered into agreements and have established external authority structures to regain some control over these increasing trans-border flows resulting from globalization (Keohane R. O., After Hegenomy: Cooperation and Discord in the World Political Economy, 1984; Krasner S. D., 1999). Thereby trading in some of their personal authority and autonomy for increased trans-border flow control.

International legal sovereignty is mostly concerned with establishing recognition for a political entity within the international system. Because the recognition within the larger international system provides both material and normative benefits, international legal sovereignty has become a political tool for rulers (Strang, 1996). As all recognized states have juridical equality, international legal sovereignty empowers smaller states, it also provides legitimacy to the ruling party domestically. Hereby economic and diplomatic discourse between states is strengthened by recognition and provides states and their subjects with a more secure status in the courts of other states. The normative rules of international legal sovereignty are not infallible however, as they pertain to a logic of appropriateness. If a state decides it is in its best interest not to follow these normative guidelines and would rather incur diplomatic penalties in favor of material gains, for example, it is free to do so.

> "[…] whatever international recognition has meant, it has not led rulers to eschew efforts to alter the domestic authority structures, policies, or even personnel of other states, or to enter into contractual relationships that compromise the autonomy of their own state. International legal sovereignty does not mean Westphalian sovereignty. Moreover, it does not guarantee that legitimate domestic authorities will be able to monitor and regulate developments within the territory of their state or flows across their borders; that is, it does not guarantee either domestic sovereignty or interdependence sovereignty." (Krasner S. D., 1999, p. 19)

Lastly, we have Westphalian sovereignty. Westphalian sovereignty rests upon territoriality and the exclusion of external actors from domestic authority structures (Krasner S. D., 1999, p. 20). Any form of intrusion in the domestic authority structures of another state, either through coercion, voluntary actions, intervention or invitation is seen as violating Westphalian sovereignty. This has resulted in a strenuous relationship with regards to the prevailing liberal international system of international legal sovereignty, which pertains that only legitimate states are subject to protection from foreign involvement in domestic affairs. What constituted legitimate in this sense is highly contested, as it has to do with the socially constructed normative logic of appropriateness and can differ widely from country to country. Either through invitation or intervention and imposition, international legal sovereignty is often used to compromise on Westphalian sovereignty. The main contribution of Westphalian sovereignty has been the establishment of the principles for legitimate rule and authority through an international agreement, cementing these principles into the hierarchical international system (Owen, 2015).

In the end, it is the dynamic between control and authority that constitutes the core of the notion of sovereignty. It also influences the perceptions of legitimate sovereignty in the current world order. Whereas control can be actively enforced, authority is a socially constructed concept that is decided upon by the rulers and the ruled, thereby providing internal legitimacy to a state's sovereignty. As the international system lacks an effective higher authority than the state, the normative adherence to authority with regards to internationally perceived legitimate sovereignty pertains to a fallible logic of appropriateness.

Addressing the Sovereignty Gap

How then do the dynamics between control and authority affect the contested notions of sovereignty in relation to the information revolution? In short, the networked nature of the globalized world, made possible by the information revolution, poses fundamental challenges to the particular notion of Westphalian sovereignty. According to political scientist and international lawyer Anne-Marie Slaughter, who tried to integrate international relations theory and international law studies and has written extensively on network theories, global networks have fundamentally challenged Westphalian sovereignty in two ways: (1) Nation-states are becoming less effective in exerting power, due to increased interdependence, and (2) adherence to Westphalian absolute sovereignty is declining, as shown by initiatives like *Responsibility to Protect*[6]. For Slaughter this means that hierarchy and control lose out to community, collaboration, and self-organization in the end (Slaughter, A New World Order, 2009). As pointed out by Miles Kahler in his work *Networked Politics*, it is no longer the nation-state, but the global financial and production networks that are the main organizing feature of markets and the dominant structures of the economy (Kahler, 2015). Both of them would agree with Owen that: "*Networks challenge the very existence and viability of hierarchical structures."* (Owen, 2015)

Building on Nye's work, Slaughter argues that power in networks lies in the ability to exert soft power. According to Slaughter authority cannot be enforced in networks, it needs to be acquired through endearment and obligation:

> "The power that flows from this type of connectivity is not the power to impose outcomes. Networks are not directed and controlled as much as they are managed and orchestrated. Multiple players are integrated into a whole that is greater than the sum of its parts – an orchestra that plays differently according to the vision of its conductor and the talent of individual musicians." (Slaughter, A New World Order, 2009, p. 99).

Sovereignty, therefore, needs a different conceptualization, one that is predicated on participation, international institutions and the organizational structure of networks. Unfortunately, as noted by Owen, whilst Slaughters network approach is a step in the right direction, it still privileges state behavior and as a result the state as the main actor in international affairs. Other actors that have been empowered by the information revolution and are not constrained by the same legal, ethical and regulatory norms as states, are left outside of this framework. Further complicating things is the fact that these new actors are not necessarily bound by personal or collective interests, making them extremely difficult to control (Owen, 2015).

As has become clear, the differing notions of sovereignty are inherently contentious, and the information revolution hasn't changed this. What the information revolution has changed is the role of the state in this regard. As with the notion of security, the state is no longer the sole or sometimes even primary structural actor in the international system, but the state has a choice in how it wants to adapt to this revolutionary turn of events (Kello, 2017). It basically leaves states with two options regarding their sovereignty, pursuing absolute control and risking its authoritative legitimacy, or giving up some sovereignty in favor of maintaining its normative and stabilizing role in international affairs (Addis, 2004;

[6] Responsibility to Protect (or R2P) was endorsed by all members of the United Nations at the 2005 World Summit and provides a framework for intervention in the case of mass atrocity crimes and human rights violations by the United Nations Security Council.

Owen, 2015). In both cases there is a strong role to play for the state, one that can either be conducive to the technological advancements of the information revolution and provide normative and moral guidance in a very disruptive sector, or one that can be enormously restrictive and strangle the emerging networked society whilst risking its own legitimacy and authority in the process.

Updating IR-theory for the Information Age

So how then do we reconcile the notions of security and sovereignty within international relations theory with the challenges posed by the information revolution? As alluded to in the previous sections, there is a choice to be made with regards to the fundamental concept of the primacy of the state in both notions. We can choose to ignore the revolutionary nature of the information age and continue along the conservative or traditional path that advocates for more stringent and static notions of security and sovereignty. However, as shown in the previous chapter, we would be constraining ourselves as both notions have been contested concepts for quite some time and increasingly fail to address and explain our current situation. This chapter will first explore the competing paths that are open to us, both of which involve considerable trade-offs. Where one option might be to dismantle the notion of sovereign states entirely, another option sees states coopting the innovations and tools that the information revolution provides to fight back and seize absolute control. Secondly, and this might seem a bit counter to my point, I will argue for the continued relevance and power of the state in international affairs albeit no longer as the sole or primary actor. Lastly, I want to put forth a different framework for international relations theory, that would require a paradigmatic shift in our views on both security and sovereignty, but better accounts for the changes brought forth by the information revolution.

Freedom versus Control

The modern hierarchal, institutional and structural form of the Westphalian state was created to deal with a specific set of problems and issues, that the largely decentralized feudal structures of previous eras were ill equipped to handle efficiently. The hierarchical and centralized structure of state institutions was the main organizational structure that could relatively efficiently tackle the economic, social, and political issues that the governance of large modern communities of people required. Creating these hierarchical organizations was relatively hard and therefore preferential to states, as they could more easily muster the resources needed for the construction of these institutions. Coincidentally, the Treaty of Westphalia established the core principles for legitimate rule – namely: sovereignty, the right to self-determination, legal equality between states, and non-intervention in the internal affairs of other states – and would set the rules for state behavior (Addis, 2004; Owen, 2015). During this period the relationship between the state and its citizens or subjects was also established by thinkers like Hobbes, Rousseau, and a little later, Weber. With Weber defining the state as having the monopoly on the legitimate use of physical force in his influential *Politik als Beruf* essay, the state was further cemented as the main political actor in international affairs (Weber, 2004). Resulting in two competing views on the state: the classical *contractarian* view, supported by Hobbes, Rousseau, and Locke, and the more contemporary *predatory* view, related to Charles Tilly's notion of "the state as organized crime" where the state acts more like a protection racket (Owen, 2015; Tilly, 1990).

Central to the contractarian view of the state is the classical notion of the "social contract" as propagated by Rousseau between the state and its subjects, that delineates the rights and responsibilities between them. The Hobbesian idea of the state of nature, which is a total state of anarchy where it is every man against every man, requires a common power to keep them all in awe (Hobbes, 1651). As Robert L. Carniero points out in his paper on *A Theory of the Origin of the State*, the contractarian view rests on a supposed voluntary relinquishment by people of certain freedoms in return for the organizational and governance capabilities a state can provide.

> "[…], at some point in their history, certain peoples spontaneously, rationally, and voluntarily gave up their individual sovereignties and united with other communities to form a larger political unit deserving to be called a state." (Carniero, 1970, p. 733)

Contrary to the contractarian view of the state as an arbiter between individual conflict and an organizational structure for communities, the predatory view rests on the coercive power of the state over its peoples. Carniero poses that war and territorial control are far more formative for state organizational structures and that increasing coercive power has been the main driver of state development. In this view, the predatory state uses its monopoly on the use of violence to enforce laws and rules on its subjects. Mainly concerned with maintaining their monopoly over violence and their own survival, the rulers of predatory states will constantly try to increase their modes of control, according to Owen. The information revolution has put this emphasis on control by the state in a paradoxical situation. Whilst its technological developments both threaten the internationally perceived legitimate sovereignty of the state, as shown in the previous chapter, it also makes possible a new type of surveillance state that has unprecedented levels of control over its inhabitants and strains the domestic legitimacy of state sovereignty.

Globalization and to a certain extent the information revolution that accompanies it has been a highly polarizing process (McCarthy, 2015). With proponents of globalization proclaiming the end of the territorial state and painting a utopian future of technological innovations that have ushered in a new era of human development, the information age. Opponents of globalization and the information revolution are less optimistic about the future of human development and advocate for the continued existence and even strengthening of the territorial state as a guardian against the more nefarious and darker sides of technological development and human nature. But in doing so, they might also give the state all the tools it needs to create a type of Orwellian surveillance state that breaks with many of the currently proselytized liberal human rights of its citizens. As Adeno Addis noted in his paper on *Sovereignty in the Information Age,* both sides fail to coherently address the tension between the technological reality and the institutional claims of the territorial state, and so misapprehend the nature of the information revolution (Addis, 2004).

In line with the optimistic view on globalization, the disruptive technologies of the information revolution have empowered individual actors into a position that now threatens to replace the dominance of existing institutions in many areas of international affairs such as development, war, diplomacy, finance, international reporting and activism (Owen, 2015). The weaknesses of the state - a lack of structure, instability, decentralized governance, loose and evolving ties – is precisely antithetical to the strengths of new digital actors in the networked world. As Manual Castells famously states: "*Power does not reside in institutions, not even the state or large corporations. It is located in the networks that structure society …"* (Castells, Afterword: why networks matter, 2004). This view is increasingly supported by globalists and others that have prophesized the end of the nation-state. Hans J. Morgenthau stated as early as 1964, that *"the sovereign nation-state is in the process of becoming obsolete"* (Morgenthau, 1964). Some globalists go even further, calling the decay of sovereign nation-states a "*positive development"* (Madison, 1998). And as Addis himself notes, it is almost cliché to say that the nation-state is on its final legs in today's globalization narrative.

It only seems logical then, that the rulers of the older hierarchical institutions feel threatened by this discourse and these new and often unaffiliated and decentralized actors entering their domain. These digitally enabled actors often have different values, objectives, and are creating new forms of organization that undermine and challenge the hierarchical foundations of many of these institutions. States are not helpless in their struggle for survival and continued monopoly over violence, however. In their quest for increased control, the new technologies of the information revolution have actually proven to be very effective tools in the predatory state's arsenal. Or as Owen puts it:

> "For a government that sought to know everything, to collect it all, corporations had built an infrastructure, and the public had filled in much of the data. The same technological system that empowers people to disrupt traditional and state institutions has been shown to be incredibly effective at providing the backbone of a surveillance state." (Owen, 2015, p. 17)

This propensity for intelligence gathering and surveillance in the digital sphere has already shown to be widely practiced by nations across the globe (Segal, 2016). From the leaking of the extensive NSA surveillance program by Edward Snowden to the implementation of the social credit system in China that digitally tracks its citizens, many states have sought to increase their control through the digital tools of the information revolution. These enormously invasive tactics come at huge material and immaterial costs though. Not only are these programs enormously expansive to run, but the sheer amount of big data that is easily collected also has to be evaluated and processed, something that has proven more difficult.

The bigger problem arises when we link these issues to the notion of the internationally perceived legitimate sovereignty of states. As noted by Addis:

> "it is not the freedom from external interference that is central to sovereignty in the information age and generally in the age of globalization, but rather the freedom to engage in the constitution of, and participation in, international institutions and norms." (Addis, 2004, p. 56)

The more predatory tactics (like those mentioned above) the state employs, the greater the strain on the supposed "social contract" between the state and its citizens. Whilst more autocratic nations like China and Russia have greater leeway in employing such tactics, democratic states are increasingly vulnerable to this erosion in the underlying foundation of democratic governance (Deibert, Palfrey, Rohozinski, & Zittrain, 2010; Deibert, Palfrey, Rohozinksi, & Zittrain, 2012; Segal, 2016). The participatory nature of democratic governance has become increasingly decoupled from actual reality as political party systems across the democratic world have atrophied. More troubling is the fact that emerging systems and actors that are brought forth and supported by the innovations of the information revolution and try to offer new solutions to these problems are delegitimized by the status-quo governance discourse (Owen, 2015; Segal, 2016). One example being the Occupy movement that advocated for more participatory governance systems and accountability, using network architecture coupled with digital communication tools to create a horizontally structured movement following the financial crisis of 2007. As David Graeber has pointed out in his work titled *The Democracy Project* that looks in-depth into the history and aftermath of the Occupy movement, the exclusion of the electorate and the handling of the crisis by the institutions and powers that be only increased the disenfranchised feeling of certain groups within society (Greaber, 2013). Eventually, this feeling of disenfranchisement has resulted in a polarized landscape that has increased instability both domestically in many democratic countries as well as internationally due to the rise of nationalism and protectionism in international politics.

Due to these rising tensions, the call for a more nationalistic approach towards the digital sphere has increased too. The option remains to carve up the internet in different territorial blocks, each subject to their individual sovereignty, or as Adam Segal puts it in his work *The Hacked World Order*: “The Balkanization of the Internet”. But that would severely undercut the usefulness that a global network provides (Harknett R. , 2003). Attempts at this have been made, the most famous one being the “Great Firewall” of China, that partitions the Chinese network from the larger internet. But as Deibert, Palfrey, Rohozinski and Zittrain argue in their work titled *Access Contested,* China is almost uniquely situated for this approach (Deibert, Palfrey, Rohozinksi, & Zittrain, 2012). As shown by the evolution of the Internet as outlined in the first chapter, the usefulness of a network increases exponentially in relation to its size. China’s immense domestic size means the effects of this partitioning are softened, but there are still gaps in the defenses when talking about security. With some work arounds, one can still easily access the wider internet from within China or gain access to the Chinese network from outside. So short of unplugging entirely from the global network and abandoning all the developments and innovations that the internet allows, security in the digital sphere will always involve some trade-offs (Singer & Friedman, 2014).

In the end, whilst absolute control over the networks produced by the information revolution is technically feasible for a nation that can muster the necessary resources to accomplish it, the results for democratic governance are eventually counterproductive. Apart from the astronomical material costs involved in monitoring and controlling cyberspace, the normative cost of losing legitimate domestic sovereignty alone can cripple democratic governance. Even if one is able to create a cornered off highly monitored network akin to the Chinese approach, it is still not impregnable to outside interference or domestic subversion. It also fails to solve the main problems in cyberspace that were discussed in the section of security, namely that of commensurability, rationality and attribution. As long as cyberspace favors offensive action, any defensive tactic will remain at a disadvantage and largely ineffective.

The moral argument for the State

Whilst the pessimistic view of the all-controlling Orwellian state is haunting, the more stringent approach to the notions of security and sovereignty in the information age, the contrarian view of total freedom in the digital sphere is equally harrowing. As Kello and Owen argue, the information revolution has brought forth a systemic change in the international order. Kello's concept of first order revolution or systems change only occurs when players alien to the system challenge the supremacy of the dominant units. Introducing new norms, values, rules of behavior and possible conflicting objectives, these new actors significantly affect the purposes of the status-quo (Kello, 2017; Owen, 2015). The sheer speed of innovation and information production in the digital realm is outpacing our collective capability to fully understand it. In this environment, certain actors that are flexible, digitally savvy and that thrive on uncertainty and confusion, have a distinct advantage. Hacktivist groups like Anonymous can run circles around lumbering institutions that require long term strategic planning to mobilize resources and draft policies. Whilst states still enjoy some supremacy in the use of high-end weaponry, like for example the development of the STUXNET[7] worm, lesser private actors outside of the state system pose highly relevant threats. Companies like Apple, Google, Microsoft and Amazon provide much of the digital infrastructure and because of this are in many ways more capable than states in taking digital actions (Kello, 2017). Therefore, from a security standpoint, it is insufficient to just focus on state relations when it comes to interactions in the digital sphere, one must also look at what happens at the lower private levels.

If we look at security specifically, we see that the lines between the private and the public sector are becoming increasingly blurred. As the Internet and the digital sphere has evolved, the role of commercial interests and private actors has increased exponentially. Not only have private companies become the main innovators in the digital sphere, but they also commercialize technologies, provide new services, defend against cyberattacks and uncover digital espionage, as showcased by the discovery of the STUXNET worm by the private security firm VirusBlokAda. States have to increasingly rely on networks owned by the private sector and this dependency not only prevents states from acting alone but also pulls them in ever more directions. This overextension of the state has meant that governments have failed to effectively protect the private sector, increasing the support in the vulnerable private sector for the use of active defense measures by companies (Segal, 2016).

The US Department of Defense describes active cyber defense as: '*[the] synchronized, real-time capability to deter, detect, analyze, and mitigate threats and vulnerabilities*' (U.S. Department of Defense, July 2011, p. 7). The problem with the use of active defense measures brings us back to the central problems regarding security questions in the digital sphere, those of attribution, commensurability and rationality. As Kesan & Hayes explain, cyberspace privileges offense actions, the *active* in active defense entails mitigative counterstriking of supposed targets (Kesan & Hayes, Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace, 2012). However, as discussed before, knowing the identity of the attacker and the severity of the attack is extremely difficult in cyberspace. These problems with attribution and commensurability can quickly escalate if left unchecked. What further confounds the problem is the rationality of private actors. Where most developed states are subject to democratic accountability and public oversight,

[7] STUXNET is believed to be a US/Israeli developed malicious computer worm, that was used to damage reportedly one fifth of Iran's nuclear centrifuges. It was discovered in 2010 and is believed to be the one of the first concerted attempts at using a digital weapon.

private companies are unconstrained by these checks and balances and answer mostly to their boards and investors. Driven by market forces, the power of the private sector poses a real threat to the pluralism and diversity of global society. As Owen, Addis, Kesan & Hayes and to a certain extend Kello point out, this is where the moral argument for the continued existence of the state might come in, as it "*may be the only institution that is capable of minimizing the international tendency to uniformize cultures and individuals."* (Addis, 2004, p. 71)

To understand this threat of uniformity imposed by technological innovation, we will have to look at technology from a more constructivist angle, as being socially constructed. Technological artifacts and tools aren't neutral objects, they are a form of institutional power that privileges some more than others. As Daniel McCarthy illustrates in his work *Power, Information, Technology and International Relations*:

> "[…] social power relations are important in the making of design choices. Levels of hierarchy or anarchy, democratic governance, legal institutionalization, and normative integration within an international system will thereby influence the types of technological institutions created at any given moment in time." (McCarthy, 2015, p. 4)

Herein lies a central role for international relations scholars in delineating and shaping the particular trajectories for technological development. Innovation doesn't happen in a vacuum, it builds on previous developments and specific policies, social norms and values shape these trajectories. Technologies, and with regards to this paper, digital technologies, in particular, are not neutral tools in and of themselves. As Owen puts it, "*They empower those who build and understand how to use them."* (Owen, 2015, p. 207). Currently that basically means Silicon Valley and the Western technology companies like Google, Apple, Microsoft and Facebook, that it has spawned and who control the majority of the digital networks we depend on for the daily functioning of society. This means that most of the innovations within cyberspace come from a very specific region, with a very specific tradition and cultural background. Making these giants of industry more accountable to the public, combating monopolies and championing inclusiveness and diversity, will be some of the main challenges facing the new role of the state as the moral gatekeeper of society.

Whilst proposing a totally new international system of governance clearly goes beyond the aspirations of this paper, I would like to purpose some possible avenues of approach. One promising solution might be the establishment of a new multilaterally agreed upon standard of norms and behaviors in cyberspace, such as proposed by Catherine Lotrionte in her essay on *State Sovereignty and Self-Defense in Cyberspace* (2012). However, the discourse on these new norms and behaviors should not be relegated solely to states, broadening the discussion to encompass the private sector will better reflect the reality of cyberspace. The role of the state would be that of arbiter and enforcer of this newly created international legal institutionalism. This reimaging of international legal sovereignty would produce clearer and more effective legislation, that better accounts for the inherent ambiguity of threats in cyberspace (Kesan & Hayes, Thinking Through Active Defense in Cyberspace, 2010; Gartzke & Lindsay, 2015). Whilst by no means being an easy feat to accomplish, the broadening of the negotiations on these issues to be more inclusive to private actors will be a small step in the right direction.

As talked about in the first section, what started out as a US Defense project has grown into something that affects all of us and permeates into every level of society. Yet as Singer & Friedman have noted, interaction with this new realm is often overlooked or ignored as a thorough understanding of its functioning is lacking in the field of governance and because of that it is too often relegated to the more technically inclined. As Adam Segal observed, policymakers have struggled to engage with the demands that cyberspace has placed on them. The "*offensive advantage, rapid technologic change, accelerating pace of communication, blurred boundaries between war and peace, the centrality of the private sector – have compounded and added to their disorientation"* according to Segal (2016, p. 469).

In the end, states will have to accommodate the information revolution if they want to remain relevant in the discussion around cyberspace and preserve the benefits that the continued access to the global network has brought. This will have to start with educating themselves on the topic of cyberspace. The disconnect between policymakers and the reality of technological developments in cyberspace has to be rapidly bridged. As Yochai Benkler states, continuing to resist engagement with the information revolution will put governments "*at odds with some of the most energetic and wired segments of society. […] Any society that commits itself to eliminating what makes Anonymous possible and powerful risks losing the openness and uncertainty that have made the Internet home to so much innovation, expression, and creativity."* (Benkler, 2012). As Owen notes, a better course of action is to embrace the disruption caused by these new developments, protect the network at all costs and support these new and empowering technologies. In doing so, the roles of the state will have to take on new forms, or as Owen puts it:

> "The contemporary international network, complex as it is, positions states in multiple roles: as producers, consumers and mediators of technology. At the center of this role lies a paradox: the tools that enable autocratic governments to monitor and control their citizens are produced by Western technology companies. States seeking an international agenda that foregrounds the individual must recognize these contradictions and ensure that they consistently act in the name of individual rights and freedoms." (Owen, 2015, p. 207)

The Network as a new framework for IR-theory

A new framework might help for incorporating the information revolution into international relations theory, one that isn't predicated on hierarchical structures like the Weberian model of organization (Harknett R. , 2003). But one that is flexible and open to new actors and more dynamic relationships on the international stage. A framework that best resembles the fundamental architecture of the globalized information society we are living in, a framework that emphasizes the network. As Manuel Castells observed in his trilogy on the Information Age:

> "Networks constitute the new social morphology of our societies, and the diffusion of the networking logic substantially modifies the operation and outcomes in processes of production, experience, power and culture. While the networking form of social organization has existed in other times and spaces, the new information

> technology paradigm provides the material basis for its pervasive expansion throughout the entire social structure." (Castells, The Information Age: Economy, Society and Culture, 2000, p. 500)

Originating in both the computer sciences and the social sciences independently, the concept of network theory and network analysis has been around for some time now but has only recently been brought into the field of international relations. As talked about previously, the neorealist focus on hierarchical structure, based on the distribution of material capabilities across actors and units within the international system has remained dominant in international relations. And networks have mostly been looked at as organizational forms alongside state hierarchies and markets. Only recently have some within the discipline of international relations treated networks as structures in and of themselves that can both constrain and enable individual agents and influence international outcomes (Hafner-Burton, Kahler, & Montgomery, 2009).

In their work *International Relations: A Network Approach* Zeev Maoz, Ranan Kuperman, Lesley Terris and Ilan Talmund make a compounding attempt at bringing network theory into the field of international relations. In it they argue that, "*social interactions in general, and international interactions, in particular, can be conceived of as a set of networks"* wherein, "*a network is a group of units bound together by a certain rule, link or other type of connection"* (Maoz, Kuperman, Terris, & Talmund, 2003, p. 3). The interactions within these networks can be described from the point of view of individual units like the individual or state, a subset of units, like the EU or NATO, or from the perspective of the entire system. Where traditional methods and theories would require us to reduce the number of issues, relations or actors we want to examine, to a familiar monadic, dyadic, or systemic level of analysis to be able to handle complex issues. A network approach allows us to examine all of them simultaneously and cumulatively, providing a more comprehensive framework of analysis (Maoz, Kuperman, Terris, & Talmund, 2003).

> "Network analysis aims to identify patterns of relationships, such as hubs, cliques, or brokers, and to link those relations with outcomes of interest. Structural relations are as important as, if not more important than, attributes of individual units for determining such outcomes. As a result, the beliefs and actions of individual agents (and observations of individual behavior) are not independent. In contrast to more static conceptions of structure, such as the neorealist variant, network relations are inherently dynamic." (Hafner-Burton, Kahler, & Montgomery, 2009, p. 561)

Some caution has to be taken here though, as the level of analysis problem within international relations does not completely disappear in a networked world, as noted by Emilie Hafner-Burton, Miles Kahler and Alexander Montgomery in their work *Network Analysis for International Relations*. Relating international relations networks between governments for example to outcomes that rely on findings from networks of individuals, often fail to demonstrate that the same mechanisms operate at a different level of analysis. The mechanisms that connect network structures to network effects need to be carefully considered and justified when changing levels of analysis between individual units, subsets or systemic conditions. For example, similar network structures have been coupled to shared identities or commonalities, yet this does not have to mean that individual nodes in similar positions act in the same way. The effects of network position on the behavior of actors must be carefully considered as well as the distinguishing network resources that are open to said actors. The differing power balance between a single person and a state still differentiates their influence and capabilities within a network, even though they might theoretically occupy a similar position within that network (Hafner-Burton, Kahler, & Montgomery, 2009).

All in all, the holistic approach of placing international relations in a network framework will allow us to better examine the problems of both security and sovereignty by incorporating both the public and the private within the same system of analysis. With the mentioned decline of state power and sovereignty in international affairs, the hierarchical structuring of the world order that was so typical of this older system has started to crumble in conjunction with this loss in the dominance of the state (Owen, 2015; Nye, Power in the Global Information Age, 2004). The network approach, if applied correctly, also addresses the level of analysis problem that plagues the multidimensional nature of security issues in international relations theory, as argued by Maoz, Kuperman, Terris and Talmund (Maoz, Kuperman, Terris, & Talmund, 2003). When used in conjuncture with Buzan, Weaver and de Wilde's concept of securitization, the focus on multidimensional relationships in international affairs from a network perspective gives a much-needed theoretical framework for analysis that is currently lacking in the divided discourse on security within international relations theory. In applying this network framework, international relations theory doesn't have to dispose of or disregard its differing theoretical schools, instead it opens up the opportunity for different schools to inform one another whilst being incorporated within a coherent metatheoretical framework. Having a clear framework helps in addressing the more pragmatic solutions that have been offered thus far for reconciling the different schools within international relations (Eriksson & Giacomello, 2006). As argued throughout this paper, the developments of the information revolution require a framework that incorporates not just the state, but also the private sector, wider social community and the individual into the theoretical units of analysis. As Hafner-Burton, Kahler and Montgomery rightfully caution against, more testing of network theory and network analysis is required to fully incorporate it into the field of international relations (Hafner-Burton, Kahler, & Montgomery, 2009). The construction of the necessary large-scale datasets will require some hard work and help from information revolution innovations and ingenuity. But the promise of a coherent all-encompassing framework that bridges the discourse within the entrenched positions of the field of international relations theory is worth investigating further.

Conclusion

The field of international relations has yet to thoroughly engage with the problems the information revolution has caused for its discipline. The sheer speed of developments has confounded and confused many policymakers and scholars within international relations. Struggling to keep pace with these developments many have opted to ignore the fundamental challenges of the information revolution, ignoring its revolutionary character and sticking to old paradigms. Only engaging with the subject matter on a policy level, without placing the technological developments in a wider theoretical framework that might explain the wider developments coherently. As Kello eloquently describes:

> “The cyber age has given rise to an expanding field of technical specialists but no true sages, students but few qualified theoreticians, policymakers yet scarcely any accomplished statesmen – it has, in brief, produced no masters.” (Kello, 2017, p. 4)

Yet it doesn’t have to be this way, as the history of the internet has shown. When the private and the public sector work together, they can do more than produce pragmatic policy. They can create a new virtual domain that has ushered in a new age for human development. Updating international relations theory for this new era will require a fundamental reconceptualization of some of its core notions, two of which I have discussed at length in this paper, the notions of security and sovereignty.

The contested notion of security reveals the fractured landscape within international relations theory that has hampered the development of a coherent framework for tackling the issues of cyberspace. Preventing policy and theory levels of analysis from actively informing one another. The different schools within international relations theory all bring something to the table. The long dominant neo-realist approach remains preoccupied with the state as the primary actor but is one of the few schools that has actually engaged with the information revolution, albeit from a mostly military perspective. Whilst the development of the model of securitization by the Copenhagen School can effectively explain how issues get securitized in cyberspace, the liberalists allow for the inclusion of the newly cyber empowered actors other than states, and constructivists do a good job at explaining the behavior of these new actors in cyberspace, yet all of them have only recently started examining cyberspace from their respective viewpoints.

As is the case with security, the notion of sovereignty has been a contested one. As the process of globalization has intensified, the notion of state sovereignty has come under increasing pressure. The conservative hold on state supremacy within international relations has been hard to break yet the information revolution has made it increasingly clearer that the position of the state as the sole actor in international relations theory has to be amended. Whilst the state is far from powerless in this new age, as shown by the increased possibilities of a strengthened surveillance state, it is far from being the only powerful force in cyberspace. The relation between the private and the public sector will have to be reexamined, which brings me to my final point: the network.

If the fractured whole that is international relations theory at the moment is to be reconstructed into a coherent narrative, it might want to look at the strengths of the networked world brought about by the information revolution. Focusing on flexible and changing relationships between nodes. In this theoretical network framework power remains the fundamental structuring force, however it is no longer situated at the end-points of the network, the actors or nodes, but it is situated in the relationships and linkages of the network itself. Participation in the network then becomes paramount to the continued relevance of not only the state, but the relevance of international relations theory too.

Bibliography

Addis, A. (2004). The Thin State in Thick State in Thick Globalism: Sovereignty in the Information Age. *Vanderbilt Journal of Transnational Law, 37*, 1-107.

Aronson, J. D., & Cowhey, P. F. (2010, March). The Information and Communication Revolution and International Relations. *Oxford Research Encyclopedia of International Studies*, 1-19.

Arquilla, J. (2003). Thinking about new security paradigms . *Contemporary Security Policy, 24*(1), 209-225.

Arquilla, J., & Ronsfeldt, D. (2001). *Networks and Netwars: The future of terror, crime and militancy.* Rand.

Benkler, Y. (2012). Hacks of Valor: Why Anonymous is not a threat to national security. *Foreign Affairs*(www.foreignaffairs.com/articles/137382/yochai- benkler/hacks-of-valor).

Borgatti, S. P., & Halgin, D. S. (2011). On Network Theory. *Organization Science, 22*(5), 1168-1181.

Buzan, B., Weaver, O., & de Wilde, J. (1998). *Security: a New Framework for Analysis.* Boulder: Lynne Rienner Publishers.

Carniero, R. L. (1970). A Theory of the Origin of the State: Traditional theories of state origins are considered and rejected in favor of a new ecological hypothesis. *Science, 169*(3947), 733-738.

Castells, M. (2000). *The Information Age: Economy, Society and Culture* (Vol. I). Oxford: Blackwell Publishers Ltd.

Castells, M. (2004). Afterword: why networks matter. *Demos Collection*, 219-225.

Castells, M. (2011). A Network Theory of Power. *International Journal of Communications, 5*, 773-787.

Castells, M., & Cardoso, G. (2006). *The Network Society: From Knowledge to Policy.* Washington, D.C.: Johns Hopkins Center for Transatlantic Relations.

Cerf, V. (n.d.). *A Brief History of the Internet & Related Networks*. Retrieved November 5, 2018, from Internet Society: https://www.internetsociety.org/internet/history-internet/brief-history-internet-related-networks

Choucri, N. (2000, July). Introduction: CyberPolitics in International Relations. *International Political Science Review, 21*(3), 243-263.

Clausewitz, C. v. (1940). *On War.* Altenmünster: Jazzybee Verlag.

Clunan, A. L., & Trinkunas, H. (2008). Ungoverned Spaces? Alternatives to State Authority in an Era of Softened Sovereignty. *ISA's 48th Annual Meeting, Bridging Multiple Divides* (pp. 1-26). San Francisco, CA: NPS Archive: Calhoun.

Deibert, R., Palfrey, J., Rohozinksi, R., & Zittrain, J. L. (2012). *Access Contested: Security, and Resistance in Asian Cyberspace.* Cambridge: The MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2010). *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace.* Cambridge: The MIT Press.

Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR)relevant Theory? *International Political Science Review, 27*(3), 221-244.

Freeman, L. (2004). *The Development of Social Network Analysis: A Study in the Sociology of Science.* Empirical Press.

Gartzke, E., & Lindsay, J. R. (2015). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Cyberspace, Security Studies, 24*(2), 316-348.

Goldman, E. (2003). Introduction: Security in the information technology age. *Contemporary Security Policy, 24*(1), 1-12.

Greaber, D. (2013). *The Democracy Project: A History, A Crisis, A Movement.* New York: Spiegel & Grau.

Hafner-Burton, E. M., Kahler, M., & Montgomery, A. H. (2009). Network Analysis for International Relations. *International Organization, 63*, 559-592.

Harknett, R. (2003). Integrated security: A strategic response to anonymity and the problem of the few. *Contemporary Security Policy, 24*(1), 13-45.

Harknett, R. J., & Stever, J. A. (2009). The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen. *Journal of Homeland Security and Emergency Management, 6*(1), 1-12.

Held, D., McGrew, A., Goldblatt, D., & Perraton, J. (1999). *Global Transformations: Politics, Economics and Culture.* Cambridge: Polity Press.

Hobbes, T. (1651). *Leviathan.* (E. White, & D. Widger, Eds.) Project Gutenberg.

Kahler, M. (2015). *Networked Politics: Agency, Power, and Governance.* Cornell University Press.

Karlgaard, R. (2003, April 28). The Big Cheap Chance. *Forbes*.

Kello, L. (2017). *The Virtual Weapon and International Order.* New Haven: Yale University Press.

Keohane, R. O. (1984). *After Hegenomy: Cooperation and Discord in the World Political Economy.* Princeton: Princeton University Press.

Keohane, R. O., & Nye, J. S. (1971). *Transnational relations in World Politics* . Cambridge: Harvard University Press.

Keohane, R., & Nye, J. (1987). Power and interdependence revisited. *International Organization, 41*(4), 725-753.

Keohane, R., & Nye, J. (1998). Power and Interdependence in the Information Age. *Foreign Affairs, 77*(5), 81-94.

Kesan, J. P., & Hayes, C. M. (2010). Thinking Through Active Defense in Cyberspace. *Proceedings of the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options* (pp. 327-341). Washington, DC: National Academies Press.

Kesan, J. P., & Hayes, C. M. (2012). Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace. *Harvard Journal of Law & Technology, 25*(2), 431-543.

Kissinger, H. (2014). *World Order: Reflections on the Character of Nations and the Course of History.* New York: Penguin Press.

Krasner, S. D. (1999). *Sovereignty: Organized Hypocrisy.* Princeton: Princeton University Press.

Krasner, S. D. (2009). *Power, the State, and Sovereignty: essays on international relations.* London: Routledge.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., . . . Wolff, S. (1997). *A Brief History of the Internet*. Retrieved november 05, 2018, from Internet Hall of Fame: https://www.internethalloffame.org/brief-history-internet

Lord, K. M. (2006). *The Perils and Promise of Global Transparency.* Albany: State University of New York Press.

Lotrionte, C. (2012). State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights. *Emory International Law Review, 26*, 825-919.

Madison, G. (1998). *Globalization: Challanges and Opportunities.* Hamilton: McMaster University's Institute on Globalization and the Human Condition.

Maoz, Z., Kuperman, R. D., Terris, L., & Talmund, I. (2003). International Relations: A network approach. *Gilman Conference on New Directions in International Relations.* Yale University February 21-23: ResearchGate.

McCabe, M. B. (2013). U.S. Hispanics Go Mobile: Adoption and Marketing Engagement Trends. *International Journal of Mobile Marketing, 8*(2), 67-74.

McCarthy, D. R. (2015). *Power, Information, Technology and International Relations Theory.* London: Pallgrave Macmillan.

Mearsheimer, J. J. (1983). *Conventional Deterrence.* Ithaca: Cornell Univeristy Press.

Mingus, C. M. (2013). *Clausewitz and the Analytical Cultural Framework for Strategy and Policy.* Carlisle: United States Army War College.

Moore, G. E. (1998). Cramming More Components onto Integrated Circuits. *Proceedings of the IEEE, 86*(1), 82-85.

Morgenthau, H. J. (1964). The Intellectual and Political Functions of a Theory of International Relations. In H. Harrison, & ed., *The Role of Theory in International Relations.* Princeton: Van Nostrand.

Nye, J. (1990). Soft Power. *Foreign Policy, Twentieth Anniversary*(80), 153-171.

Nye, J. (2004). *Power in the Global Information Age.* London: Routledge.

Owen, T. (2015). *Disruptive Power: The Crisis of the State in the Digital Age.* Oxford: Oxford University Press.

Rainie, L., & Wellman, B. (2012). *Networked: The New Social Operating System.* Cambridge: MIT Press.

Rayward, W. B. (2014). Information Revolutions, the Information Society, and the Future of the History of Information Science. *Library Trends, 62*(3), 681-713.

Scott, J. P. (2000). *Social Network Analysis: A Handbook.* Thousand Oaks : Sage Publications.

Segal, A. (2016). *The Hacked World Order.* New York: PublicAffairs.

Singer, P., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What everyone needs to know .* New York: Oxford University Press.

Singh, J. P. (2013). Information Technologies, Meta-power, and Transformations in Global Politics. *International Studies Review , 15*, 5-29.

Slaughter, A.-M. (2009). *A New World Order.* Princeton: Princeton University Press.

Slaughter, A.-M. (2009). America's Edge: Power in the Networked Century. *Foreign Affairs*, 94-113.

Stockinger, H. (2007). Defining the grid: a snapshot on the current view. *The Journal of Supercomputing, 42*(1), 3-17.

Strang, D. (1996). Contested Sovereignty: The Social Construction of Colonial Imperialism. In T. Biersteker, & C. Weber, *State Sovereignty as a Social Construct* (pp. 22-49). Cambridge: Cambridge University Press.

Stritzel, H. (2007). Towards a Theory of Securitization: Copenhagen and Beyond. *European Journal of International Relations, 13*(3), 357-383.

Sugden, R. (1989). Spontaneous Order. *Journal of Economic Perspectives, 3*(4), 85-97.

Tilly, C. (1990). *Coercion, Capital, and European States: AD 990–1992.* Cambridge: Blackwell.

U.S. Department of Defense. (July 2011). *Department of Defense Strategy for Operating in Cyberspace.* Washington, D.C.

Van Dijk, J. A. (1999). The one-dimensional network society of Manuel Castells. *New Media & Society, 1*(1), 127-138.

Waever, O. (1995). Securitization and Desecuritization. In R. L. (ed.), *On Security.* New York: Columbia University Press.

Walt, S. M. (1985). Alliance Formation and the Balance of World Power. *International Security, 9*(4), 3-43.

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

Wasserman, S., & Faust, K. (1994). *Social Network Analysis: Methods and Applications.* Cambridge: Cambridge University Press.

Weber, M. (2004). *The Vocation Lectures.* (D. S. Owen, & T. B. Strong, Eds.) Cambridge: Hackett Publishing Company.

Wendt, A. (1999). *Social Theory of International Politics.* Cambridge: Cambridge University Press.

Williams, M. (2003). Words, Images, Enemies: Securitization and International Politics. *International Studies Quarterly, 47*(4), 511-531.

Total word count: 16240