CHARLES UNIVERSITY

Between Defence and Offence: An Analysis of the US "Cyber Strategic Culture"

July 2018

2283812
71179134

Presented in partial fulfilment of the requirement for the Degree of MSc International Security, Intelligence and Strategic Studies (SECINTEL)

Word Count: 23,560
Supervisor UofG: Andrew Hoskins
Supervisor Charles Uni: Vít Střítecký

Abstract

The present thesis deals with the US strategic approach and posture to cybersecurity from a national point of view. On such a topic much has been written already, nonetheless the present work finds a degree of originality by tackling such object of analysis shifting the focus to a ideational perspective. By drawing insights from the meta-theory of Constructivism and the rich research tradition on strategic culture, the present thesis aims at understanding what kind of norms seem to be informing/mirroring what has been labelled the US "cyber strategic culture", and if it is possible to speak of a "shift", or at least track an evolution regarding them, in a historical timeframe that runs from the early 2000s up to the present days. To pursue the stated research agenda, a methodology grounded in discourse and thematic analysis is utilised, with an analytical framework centred around two opposite "thematic normative categories" (themes) called "defensiveness" and "offensiveness", each characterised by a "story" made up by three sub-themes, delineating specific strategic behaviours. A set of official strategies, all tackling cybersecurity and published during the mentioned timeframe by both the White House and the military, form the primary sources to which such methodology is applied, with particular focus being posed to the defensive paradigm known as "active cyber defence" measures, the 2015 Department of Defense's Cyber Strategy, and the 2017 National Security Strategy. Overall, it is argued that, despite a predominant presence of the theme of "defensiveness", it is indeed possible to speak of an on-going evolution, especially since 2011, which sees the norm of "offensiveness" increasingly informing the US "cyber strategic culture".

Table of contents

Acronyms

ACD	Active Cyber Defence
APT	Advanced Persistent Threat
CIP	Critical Infrastructure Protection
CNCI	Comprehensive National Cybersecurity Initiative
CNE	Computer Network Exploitation
CYBERCOM	Cyber Command
DARPA	Defense Advanced Research Projects Agency
DCEO	Defensive Cyber Effect Operation
DCO	Defensive Cyber Operation
DHS	Department of Homeland Security
DOD	Department of Defense
DODIN	Department of Defense Information Network
FOIA	Freedom of Information Act
IC	Intelligence Community
ICT	Information Communication Technology
IDM	Intrusion Detection Measure
IDP	Intrusion Detection System
IPS	Intrusion Prevention System
IR	International Relations
IS	Islamic State
JCC	Joint Concept on Cyberspace
NCDM	Non-Intrusive Defensive Countermeasure
NMS	National Military Strategy
NSA	National Security Agency
NSS	National Security Strategy
OCEO	Offensive Cyber Effect Operation

PPD-20	Presidential Policy Directive No. 20
PPD-21	Presidential Policy Directive No. 21
PPP	Public Private Partnership
RA	Response Action
RMA	Revolution in Military Affairs
STRATCOM	Strategic Command
US	United States

1. Introduction

The central object of analysis of the present dissertation is the United States' (US) approach to cybersecurity, the practice of securing so-called cyberspace, the virtual global domain, or network, societies are growingly becoming dependent of. The "cyber revolution", next to all the positive effects, also brought various negative ones, since it opened the door to a rather vast and new universe of threats and risks. With societies growing increasingly dependent on such a digital medium, achieving security from the menaces spawning within it has become a rather central topic and goal within the political and decision-making circles of many countries around the world. Accordingly, the practice of cybersecurity has achieved a rather high spot on the security agenda of many nation states. This sparked the publication of various official documents that either are partially or entirely dedicated to such practice and security need. Indeed, sections dedicated to the security of the cyber medium, and related infrastructure and information stored within it, are finding a place in official documents published by various governmental organisations.[1] In addition to that, the cyber medium has become yet another arena where international actors project their interests and power, replicating those inter-state behaviours that since quite recently were confined to more common domains. Yet again, also discussion on the posture and potential behaviour to maintain

[1] Agnija Tumkevič, "Cybersecurity in Central Eastern Europe: From Identifying Risks to Countering Threats", *Baltic Journal of Political Science*, No. 5 (December, 2016), 73 - 88, 73.

and signal to other states are now finding broader spaces within the mentioned official texts. Precisely the importance given to securing the cyber medium and states projecting their social behaviours onto it is what has been driving a change regarding the kind of research undertaken on it. Whether initially studies regarding cybersecurity and the cyber medium were somewhat confined within experts of computer science and engineering, not too long ago new research agendas have been set up and pursued, among others, by scholars of sociology, philosophy, and especially of international relations (IR) and security studies. Given the centrality the cyber medium has reached regarding the security of states and their mutual relationships, analysing their approaches to it is key to understand future possible scenarios on the evolution and exploitation of the medium itself, as well as on states' strategic behaviours. Given the highly volatile nature of cyberspace, being a man-made domain, and a perceived shared idea of policy-making and research always lagging behind a rapid and constant evolution not only of the medium, but also of the threats and risks arising from it, keep on pursuing research agendas centred around such issues is crucial.

The present thesis finds a place in, and builds a bridge with, the research agendas pursued by scholars of security studies. Despite already a rather vast body of knowledge has been created on the US strategic approach to cyber-related matters and affairs, the present thesis seeks to humbly further push such knowledge forward. Starting from a cautious and non-critical Constructivist point of view, utilising some tenets from the tradition of strategic culture studies, the present thesis seeks to analyse such actor's

approach from a more ideational and interpretative perspective. By focusing the "militarization" historical moment of the "cyber era", attention is posed to the norms that seem to be informing/mirroring the policies and signalled behaviour. To do so, the analysis of discourse, coupled with that of themes is utilised as the main methodology, in building a particular analytical framework through which the gathered primary sources are analysed. In addition, many insights are also drawn from a rich pool of gathered and scrutinised secondary sources. Overall, the intention is to assess whether the US seems to be informed more by a defensive or offensive normative background. In doing so, drawing many insights from various literary entries, the present thesis seeks to understand whether it is possible to speak of a shift, or at least track an evolution of the US "cyber strategic culture", a concept coined in the present thesis. Among the not too vast pool of primary sources gathered, great emphasis is given to some specific empirical data, precisely the discourse and nature linked to the defensive paradigm known as "active cyber defence" (ACD) measures, the 2015 Department of Defense's (DOD) Cyber Strategy, and the latest National Security Strategy (NSS), published in late 2017.

Precisely the focus given to ACD is what makes the present work stand out within the literature. Indeed, an on-going debate exists among cybersecurity experts, policy-makers, lawyers, and diplomats from various countries, regarding the strategic and legal applicability of such defensive paradigm, as well as its conceptualisation. Given that supporters attribute to ACD a high strategic value, but sceptics point out various legal gaps in its applicability, as well as arguing against such added value, the debate is long

from seeing an end, something that makes the study and analysis of ACD rather topical and of extreme interests.

Regarding its structure, the present dissertation follows a rather standard research path. Initially, a review of pertinent literary entries is presented, with also the historical context the thesis takes as point of analysis briefly explained. Secondly, overviews of both the meta-theoretical approach and research tradition the dissertation draws insights from, namely Constructivism and strategic culture, are presented. Thirdly, a discussion on the nature of the sources utilised and role both discourse and thematic analyses play within the thesis follows. Fourthly, having built such a rich literary, theoretical, and methodological background, the analytical framework through which the gathered primary sources are analysed is presented. In other words, the two normative “themes" that guide the analysis are described and their “stories” explained. Then finally, the actual analysis is carried out, focusing first on one theme and then on the other, and especially on the above-mentioned empirical proofs. Indeed, central to the overall thesis’ argument is the interpretation and thorough analysis carried out regarding the concept and conceptualisation of ACD both at a broader level and within the US, as well as the discourse and “themes” found within the two cited official strategies.

2. Literature review and historical context of the thesis

As stated in the introductory chapter, the present dissertation aims at analysing the US "cyber strategic culture" by focusing on the discourse found in some specific official documents. Before moving onto the theoretical background and methodology the present dissertation is grounded on, or at least from which its draws some insights and inspiration, it is crucial to understand what the literature has already studied and argued on issues of interest to the present thesis.

It goes without saying that the literature on cybersecurity, cyber defence, cyber war etc. is a rather vast one, with writings being published by scholars of various backgrounds. Started as a rather exclusive field for experts of computer science and engineering, with the expansion of the Internet and cyber medium, its exploitation by militaries and non-state actors, and the increased reliance of contemporary societies on it, such field of study became of extreme interest also for scholars of social sciences, and especially of IR, security, and strategic studies. Despite the present thesis deriving valuable insights and knowledge from both such "strands", technical and social, in the present chapter only some specific entries from the second one are presented, since the thesis itself finds a place in it. Initially, focus is posed on works focused on the study of the "cyber discourse"; secondly, the historical context the present thesis takes into account is presented; thirdly, some writings taking as primary sources the same ones as the present dissertation are analysed; and finally, light is shed on the thesis' originality and "gap" it seeks to fill.

2.1. Discourse analyses in regards of cyberspace and cyber-related threats and risks

Despite an argument having been made some time ago regarding the lack of a political science literature on cybersecurity rooted in theories of IR,[2] during the last decade many scholars coming from such field of research, as well as from security and strategic studies, started closing such gap, with an increasing number of books and articles, applying some specific theories derived from such scholarships, being published in various important academic journals. One key body of literature is rooted in a methodology centred around the study of the discourse adopted within the broader cybersecurity and related sub-topics, cyberwar, cyberterrorism, and cybercrime. Nowadays, there is indeed a vast literature that deals with the discourse and the power it has in creating specific realities and threats, as well as in highlighting remedies to them.

Many scholars informed by the theoretical traditions of constructivism, "securitization theory", and post-structuralism have analysed the discourse of political actors and media, underlying a wide adoption of specific analogies, words, metaphors, and expressions to frame the various cyber-related actors, threats and risks; also arguing that it has been delivered to create the link between the cyber-dimension and national security. Overall, from a rather critical perspective, the literature has demonstrated

[2] Johan Eriksson and Giampiero Giacomello, Eds., *International Relations and Security in the Digital Age* (London: Routledge, 2007), 3; Myriam Cavelty Dunn, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse", *International Studies* Review, Vol. 15, No. 1 (2013), 105 - 122, 106.

the existence of a tendency to over-inflate threats, which are often placed under the umbrella of cyberwar; a move then used to justify the adoption of specific measures and policies rather than others.[3] In the following paragraphs focus is posed exclusively on a rather little sample of such a vast literature, precisely on works that somewhat adopt a discourse analysis as their methodology, which is of interest for the present dissertation. Despite their great academic value, various publications dealing exclusively with cybercrime and cyberterrorism have not been taken in account.

A rather prominent voice is that of Cavelty Dunn whose works focus both on a broader cybersecurity discourse, as well as on the evolution and peculiarities on that found within the US.

One of her most important publication is *Cyber-Security and Threat Politics: US efforts to secure the information age*, which despite being

[3] Ralf Bendrath, "The Cyberwar Debate: Perception and Politics in U.S. Critical Infrastructure Protection", in *The Internet and the Changing Face of International Relations and Security*, edited by Andreas Wenger, *Information & Security: An International Journal*, Vol. 7 (2001), 80 - 103; Ralf Bendrath, "The American Cyber-Angst and the Real World—Any Link?", in *Bombs and Bandwidth: The Emerging Relationship between Information Technology and Security,* edited by Robert Latham (New York: Free Press, 2003), 49 - 73; Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: USA Efforts to Secure the Information Age* (New York: Routledge, 2007); Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly*, Vol. 53, No. 4 (2009), 1155 - 1175; Jerry Brito and Tate Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy", *Harvard National Security Journal*, Vol. 3, No. 1 (2011), 39 - 84; Sean Lawson, "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats", *Journal of Information Technology & Politics*, Vol. 10, No. 1 (2013), 86 - 103; Tim Stevens, "Apocalyptic Visions: Cyber War and the Politics of Time", *SSRN* (April 25, 2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2256370.

somewhat old now, being initially released in 2007, offers great historical and analytical insights on the evolution of the debate regarding cybersecurity between the mid-1980s and the early years of the 2000s that took place within the US. Adopting a "semi-constructivist stance" grounded within the Copenhagen school's "securitization theory", Cavelty Dunn utilises a methodology centred on the study of discourse, as in threat frames. According to her, "[t]hreat framing refers to the process whereby particular agents develop specific interpretive schemas about what should be regarded as a threat or risk, how to respond to this threat, and who is responsible for it".[4] Her book is mainly devoted to the analysis of how particular understanding of the reality open up the door to particular behaviour, or in other words how through them social action is influenced.[5] More in detail, Cavelty Dunn clarifies that three type of framing exist: the first one is called "diagnostic framing", which is linked to the designation of what or who is threatening and of the referent object perceived as being threatened; the second one is known as "prognostic framing", being characterised by the offered solutions to the perceived threats and by those strategies, tactics, and objectives said useful to achieve them; and finally, the third one called "motivational framing" is all about gathering consent for the stated/decided cause/action.[6]

In her analysis, Cavelty Dunn uncovers that one particular threat frame regarding computers and networks, which maintained a degree of

---

[4] Dunn Cavelty, *Cyber-Security and Threat Politics*, 8.

[5] Myriam Dunn Cavelty, "Cyber-Terror - Looming Threat or Phantom Menace?: The Framing of the US Cyber-Threat Debate", *Journal of Information Technology & Politics*, Vol. 4, No. 1 (2008), 19 - 36, 23.

[6] Ibid.

contemporaneity, solidified during the Clinton administration in the second half the 1990s. Such a frame is characterised by a focus on a rather vague notion of critical infrastructures, understood as the referent object of security that must be secured from rather vaguely defined internal and external threats.[7]

One of the most important take aways from such an analysis is the fact that, despite the "cyber-discourse" being characterised by a national connotation, until the early 2000s the role of the military in defending the US was rather limited. A conclusion in line with the work of Bendrath who, analysing the debate on cyber risks that developed in the US during the 1990s, speaks of a "failed securitisation".[8] This is crucial, since with the new millennium this started changing, as better explained later on. Further, the book already points out the usage of so-called cyber doom scenarios by certain US state officials, a topic further reprised by other scholars interested in the US "cyber discourse". Finally, of interest for the present thesis, is the fact that, already before the time-frame taken under scrutiny in it, critical infrastructures were (despite vaguely) defined as key referent object, a characteristic that persisted through time, as further pointed out by the literature and in the present dissertation.

In more recent work, Cavelty Dunn clarifies further that since the 1990s the "cyber discourse" found within the US has been characterised by the presence of three interrelated and mutual reinforcing different

[7] Dunn Cavelty, *Cyber-Security and Threat Politics*, 132.
[8] Bendrath, "The Cyberwar Debate: Perception and Politics in U.S. Critical Infrastructure Protection".

"alternatives". These are respectively called "technical", "crime-espionage", and "military/civil defence", all characterised by specific malicious actors, threats, and "referent objects". For instance, while the first one is more of a technical nature, concerned mostly with malicious software and system intrusion, and the second one more focused on so-called cyber crime and cyber espionage, the third one appears to be more "discourse driven" and linked to a national security level, adopted initially by the military and focused on matters linked to war, as well as on (the already mentioned) protection of (digital) critical infrastructure(s).[9]

In her publications posthumous to *Cyber-Security and Threat Politics*, Cavelty Dunn still adopts a rather critical stance, further arguing how "particular ways of framing threats or risks are not only a matter of choice […] but also come with political and social effect".[10] Indeed, she contends that the mentioned three US "cyber discourses", until the first half of the first decade of the 21st century, produced a rather well-balanced set of policies, with the military still not having a predominant role in defending the "homeland" and its critical infrastructures. Such a situation started to change as soon as more emphasis was given to the third discourse, the "military and civil defence" one, which started gaining more traction on the wave of a shift in the overall threat perception concerning cyber-risk

[9] Myriam Dunn Cavelty, "The Militarisation of Cyberspace: Why Less May Be Better", in *2012 4th International Conference on Cyber Conflict*, edited by C. Czosseck, R. Ottis, and K. Ziolkowski (Talinn, Estonia: NATO CCD COE Publications, 2012), 141 - 153, 142; Myriam Dunn Cavelty, "Like a phoenix from the ashes: The reinvention of critical infrastructure protection as distributed security", in *Securing 'the Homeland': Critical Infrastructure, Risk and (In) Security*, edited by Myriam Dunn Cavelty and Kristian Søby Kristensen (Routledge, 1st edition June 18, 2008), 40 - 62.

[10] Dunn Cavelty, "The Militarisation of Cyberspace", 142.

and vulnerabilities, characterised by the perception of the US being constantly and increasingly "under fire".[11]

Other scholars approached the evolution regarding the practices and measures adopted in pursuit of enhancing national cybersecurity, adopting a methodology and theoretical background similar to those employed by Cavelty Dunn, thus posing attention to the discourse and threat-framing practices to justify specific political decisions. For example, Lawson, writing from a critical constructivist theoretical point of view, focuses attention to some cyber-doom scenarios utilised within the US "cyber-discourse", such as "cyber-9/11" and "cyber-Katrina". By placing them within the context of the history of technology, military history, and the sociology of disaster, Lawson argues that the story and narrative contained in such "end-of-the-world-visions" are linked to longstanding fears of technology pessimism and technology failure, which are not really realistic. [12] Further, he contends that "[i]n cyber-doom scenarios, cybersecurity is framed primarily in terms of "war" and,[…] large-scale "disaster"[, which] can lead to a militarist, command-and-control mindset that is ultimately counterproductive". [13] Lawson's analysis does find a link with that of Cavelty Dunn since it also adopts threat framing, highlighting how cyber-doom scenarios have the potential to concretise some negative political

[11] Ibid.

[12] Of a similar note is Lewis who stresses how scenarios and coincidences utilised when crafting a linkage between cyberattacks and WMD effects are simply not credible. James A. Lewis, *Conflict and Negotiation in Cyberspace* (Center for Strategic & International Studies, February, 2013), 58.

[13] Lawson, "Beyond Cyber-Doom", 95.

choices when utilised as motivational frames, sometimes even replacing more properly formulated diagnostic frames.[14]

Similarly, Brito and Watkins focus on some threat inflation practices carried out by exponents of the US federal government, military, and media. Despite not specifying any theoretical background similar to those employed by Cavelty Dunn or Lawson, the analysis conducted by them finds a link with the ones above-mentioned, since it focuses on the potential the adoption of a certain discourse has in justifying specific policies said to be misguided. To develop their argument such two scholars pose attention to various official documents published by federal bodies, a think thank, and singular political figures between 2009 and 2010. What they uncover is the already mentioned trend to over-inflate threats coming from cyberspace, calling for more involvement of the federal government and increased spending; a rhetoric then simply picked up and re-proposed by some well-known media outlets.[15] Overall, it could be said that their analysis does find a link with the theory of "securitization" since attention is posed to "speech acts" made by figures occupying places of power that can be understood as "securitizing actors",[16] as well as with an article written by Cavelty Dunn proposing an analysis of the broader "cyber discourse", taking into account not only "elite personalities", but also other non-governmental actors who are said to "play a substantial part in constructing discursive settings".[17]

---

[14] Ibid., 99.

[15] Brito and Watkins, "Loving the Cyber Bomb?".

[16] Barry Buzan and Lene Hansen, *The Evolution of International Security Studies* (Cambridge University Press, 2009), 214.

[17] Dunn Cavelty, "From Cyber-Bombs to Political Fallout", 118.

These cited works are important not only because they give an overview on the kind of theories and methodologies adopted when analysing the "cyber discourse" within the US, but also because they introduce the time-frame (thus context) under scrutiny in the present dissertation.

2.2. The historical moment taken into account - "Militarization"

The process of militarisation indicates a "growing pressures on governments and their armed forces to develop the capacity to fight and win wars in [a particular] domain".[18] Many agree on the fact that the US, as well as many other states, is currently going through it regarding cyberspace and cybersecurity.

For instance, Haizler opens his article "The United States' Cyber Warfare History" by clearly dividing the history of US cyber warfare into three different moments, respectively labelled "Realization", "Takeoff", and "Militarization",[19] each characterised by the adoption of different doctrines and the kind of threats and adversaries faced. Whether the first two time frames, "Realization" and "Takeoff", encompass the 1980s, 1990s, and early years of the 2000s, it is the "Militarization" one that of most importance for

[18] Bulletin of the Atomic Scientists, "Ronald Deibert: Tracking the emerging arms race in cyberspace", *Bulletin of the Atomic Scientists*, Vol. 67, No. 1 (2011), 1 - 8, 2.

[19] A similar distinction is made also by Healey. Jason Healey and Karl Grindal, Eds., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Cyber Conflict Studies Association, 2013).

the present dissertation. Such phase is indeed said to begin around 2003/2004, with the semi-official conceptualisation of the cyber medium as a "new theatre of operations",[20] and still on-going. Rather than diving into explanations of the driving forces of such a process, Haizler offers a detailed description on the characteristic of the US approach to cybersecurity, highlighting governmental bodies in charge of it, focusing especially on the role of the Intelligence Community (IC) and that of the Department of Defense (DOD).[21] Overall, Haizler's article clearly demonstrates that the present thesis, given the fact that it focuses on a historical timeframe that begins with the early 2000s and goes all the way to the present days, is fully linked to the on-going process of militarisation. Accordingly, the argument of the present writing needs to be read having in mind the characteristics of such historical moment, which are briefly highlighted in the following paragraphs.

Regarding the causes that sparked and further alimented the militarisation process especially in the US some scholars adopting more traditional materialistic and rationalist IR theories, underline the strategic advantages that the cyber domain offers relative to "land, air, and sea [and especially] its asymmetric nature, plausible deniability, and [most of all] offensive

---

[20] Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?", *International Political Science Review*, Vol. 27, No. 3 (July, 2006), 221 - 244, 231; David Barnard-Wills and Debi Ashenden, "Securing Virtual Space: Cyber War, Cyber Terror, and Risk", *Space and Culture*, Vol. 15, No. 2 (2012), 110 - 123, 114.
[21] Omry Haizler, "The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking", *Cyber, Intelligence, and Security*, Vol. 1, No.1 (January, 2017), 31 - 45.

advantage";[22] arguably, all factors grasped within the US federal bodies, as showed later on.

As already mentioned, those scholars who focus on the analysis of the discourse and threat framing processes, argue that precisely a shift in such a framing and related discourses formed the basis onto which US political and military elite justified the increased involvement of the federal government and military within national cybersecurity protection, which since the early 2000s had fallen mainly within the hands of the private sector, with the role of the government and especially military limited to the protection of their own digital assets.[23] More precisely, it has been argued that the rising dependence of societies on Information Communication Technology (ICT) "introduces an existential threat that [could] be exploited [also] by states […] thus requir[ing] cyberspace to be secured".[24] Cavelty Dunn indeed explains that states now are driven by a willingness to apply a more traditional conception of border to cyberspace,[25] being thus able to define a space that needs to be secured from a variety of threats, which need to be kept out.[26] Accordingly, cybersecurity is paralleled to traditional types of threat faced by societies,

---

[22] Miguel Alberto N. Gomez, "Arming Cyberspace: The Militarization of a Virtual Domain", *Global Security and Intelligence Studies*, Vol. 1, No. 2 (Spring, 2016), 42 - 65, 43; Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends", *Strategic Analysis*, Vol. 34, No. 1 (2010), 62 - 73; Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War", *Journal of Strategic Studies,* Vol. 35, No. 3 (2012), 401 - 428.

[23] Dunn Cavelty, "The Militarisation of Cyberspace", 145.

[24] Gomez, "Arming Cyberspace", 43.

[25] Such a concept is a rather ambiguous one within cyberspace, as later on briefly explained.

[26] Such a point is further reprised in the thesis.

calling for an active involvement of the military through a discourse characterised by terms such as "defence" and "deterrence".[27] Regarding the US, the logic of deterrence has also been fully applied to cyberspace, with politicians and military officials, despite scepticism being raised by academics, thinking in such terms also regarding cybersecurity and cyber threats.[28]

Further, Cavelty Dunn also clarifies that five developments participated in speeding up the militarisation process, which are respectively linked to: the nature of so-called malware (a term better explained later on); the rivalry between the US and China; the activity of "hacktivists"; the (already stated) widely adoption of the term cyberwar when speaking of cyber-related incidents and attacks; and the 2010 discovery of Stuxnet.[29]

Whether during the two previous "cyber-eras" few international actors possessed truly advanced cyber capabilities, nowadays many more states, both major and minor within the international arena, do have them.

---

[27] Myriam Dunn Cavelty, "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities", *Science and Engineering Ethics*, Vol. 20, No. 3 (September, 2014), 701 - 715, 708.

[28] Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace", *International Security*, Vol. 41, No. 3 (Winter, 2016/2017), 44 - 71, 65.

[29] Myriam Dunn Cavelty, "The militarisation of cyber security as a source of global tension", in *Strategic Trends 2012: Key Developments in Global Affairs*, edited by Daniel Möckli (Center for Security Studies ETH Zurich, 2012), 103 - 124, 107 - 112. Arguably, also other cyber-related events and incidents that happened during the last decade had a similar effect to the ones Stuxnet had, such as the campaign of cyberattacks unleashed allegedly by Russia against Estonia's systems, as well as a similar one that happened during the conflict between Georgia and Russia the year after, in 2008. For a rather complete overview on such two events and on Stuxnet (on which a vast literature exists) see: Healey and Grindal, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*.

Secondly, as already hinted, China has been singled out as cyber-enemy no.1 by the US, with Russia, Iran, and North Korea coming right after on the list. Thirdly, cyber attacks and the means employed allegedly became more complex, targeted, and persistent.[30] Fourthly, the world saw the manifestation of some "cyber events", which had various effects (both political and organisational) at the global level. Precisely Stuxnet, a malicious software unleashed by the US and Israel against an Iranian facility devoted to the enrichment of the uranium, has been singled out as a game changer, said to have established a new norm of conduct in cyber affairs.[31] Stuxnet, as previously briefly introduced, was a wake-up call, with states not only realising the potential the cyber medium holds in enhancing their hard power capabilities, but also better visualising the threats and risks societies and militaries face. Overall, states started focusing more on offensive capabilities, sparking an arms race and fostering a "(cyber) security-dilemma"; they increased their spending in cybersecurity and

[30] Within the literature great emphasis has been given to so-called "Advanced Persistent Threats (APTs). They are described as being "stealthy, targeted, and data focused"; proper cyber campaigns designed to achieve an undetected presence within targeted networks and computers for as long as possible, deployed to steal information often deemed of such sensible nature to be linked to national security itself. Overall, APTs were indeed initially conceived by the US DOD to describe Chinese cyber-espionage efforts against US national security interests. Eric Cole, *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization* (Syngress, 2012); Ivo Friedberg, Florian Skopik, Giuseppe Settanni, and Roman Fiedler, "Combating advanced persistent threats: From network event correlation to incident detection", *Computers & Security*, Vol. 48 (February, 2015), 35 - 57; Ronald Mendell, "Advanced persistent threat" (APT), *Encyclopædia Britannica Inc.*, December 10, 2015 (accessed March 2018), https://www.britannica.com/topic/advanced-persistent-threat.

[31] James P. Farwell and Rafal Rohozinski, "The New Reality of Cyber War", *Survival*, Vol. 54, No. 4 (2012), 107 - 120.

cyber capabilities, feeding an ever increasing "cyber industrial complex", and they started setting up so-called cyber commands.[32] Regarding the US, such a kind of organisation is the so-called CYBERCOM (acronym for Cyber Command, indeed). More in detail, CYBERCOM is one of DOD's ten unified commands, which brings together all those US military components somewhat linked to cyber issues. CYBERCOM was created in 2009 as a sub-unified command within the broader US Strategic Command (STRATCOM), and placed next to the US National Security Agency (NSA) at Fort George G. Meade, in Maryland.[33] Recently, CYBERCOM's status was elevated to full independent unified combatant command, no longer directly linked to the NSA itself.[34] Overall, scholars have pointed out that a tendency to go offensive in cyberspace is reflected in such new organisation, since its mission not only involves defensive operations, but also requires it to be prepared to, "when directed, conduct full-spectrum military cyberspace operations".[35]

---

[32] Dunn Cavelty, "The Militarisation of Cyberspace"

[33] Steve Winterfeld and Jason Andress, *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice* (Syngress, 2013), 34; P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know®* (Oxford University Press, 1st edition, January 3, 2014), 133 - 138.

[34] Katie Lange, "Cybercom Becomes DoD's 10th Unified Combatant Command", *DoDLive*, May 3, 2018 (accessed June 2018), http://www.dodlive.mil/2018/05/03/cybercom-to-become-dods-10th-unified-combatant-command/.

[35] Peter Beaumont, "US appoints first cyber warfare general", *The Guardian*, May 23, 2010 (accessed May 2018), https://www.theguardian.com/world/2010/may/23/us-appoints-cyber-warfare-general; Ilai Saltzman, "Cyber Posturing and the Offense-Defense Balance", *Contemporary Security Policy*, Vol. 34, No. 1 (2013), 40 - 63, 48.

As already introduced, currently there is a widely shared belief that offence trumps defence in cyberspace. Despite such a belief being present since the 1980s, scholars from IR, security and strategic studies, have systematically been writing on it since only quite recently, again often adopting more materialist and rationalist IR theories, such as the "offence-defence balance theory". In brief, Kello clarifies that given the nature of the domain, the attackers are able to exploit defenders' vulnerabilities, achieving a high degree of unpredictability and undetectability, being also able to concentrate their resources in specific chosen procedures of entry, with the defenders needing, on the contrary, to constantly "protect the entire [and constantly growing] network surface against the vast universe of conceivable attacks".[36] Of importance for the thesis is the fact that such way of thinking regarding cyberspace has been said to be especially found in US military and political circles. Examples often cited within the literature are statements pronounced by military officials, such as former Deputy Secretary of Defense William J. Lynn III.[37] Not surprisingly, despite the high levels of secrecy, many scholars contend that the US is indeed "the most offensively capable state in cyberspace".[38]

---

[36] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", *International Security*, Vol. 38, No. 2, (Fall, 2013), 7 - 40, 27 - 28.
[37] Cited in Rebecca Slayton, "What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment", *International Security*, Vol. 41, No. 3, (Winter, 2016/2017), 72 - 109, 72.
[38] Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford University Press, 2015), 93; Brandon Valeriano and Ryan C. Maness, "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–2011", *Journal of Peace Research*, Vol. 51, No. 3 (2014), 347 - 360.

Here, a clarification is in order: despite the term “militarization" is adopted for the period beginning with 2003, with scholars often pointing out Stuxnet as the event that sparked interest in the offensive use of the cyber medium, the US military demonstrated a strategic and tactical interest for it at least since the second half of the 20th century, and especially since the 1980s and 1990s. Indeed, during the last 20 years of the last century, within US military circles, many started speaking of a ICT Revolution in Military Affairs (RMA).[39] A technology that was said of being capable of multiplying one’s own force against adversaries.[40] Strategists started publishing various manuals on such a RMA, which were put to the test during the 1991 Gulf War (within the context of Operation Desert Shield) as well as during the 1999 Kosovo War.[41] Therefore, the US military saw the turn of the millennium having already experience in the offensive use of the cyber medium, as well as a doctrine in place for such operations.

Overall, Stuxnet is often taken as the key empirical proof that the US went full offensive regarding its cyberspace capabilities, since such a malicious software was clearly developed with a specific political goal in mind, that of stopping (or at least slow down) Iran’s uranium-enrichment program,

[39] A Revolution in Military Affairs is a rather debated concept within the literature; in simple terms it can be understood as a rather dramatic change in the character and conduct of conflict due to the invention and adoption of new technologies. Some historical examples are the “gunpowder revolution” and “nuclear revolution”. Andrew F. Krepinevich, “Cavalry to computer; the pattern of military revolutions”, *The National Interest*, Vol. 37 (Fall, 1994), 30+.
[40] Bulletin of the Atomic Scientists, “Ronald Deibert”, 3.
[41] Dunn Cavelty, “The Militarisation of Cyberspace: Why Less May Be Better”, 144.

which provided it "with a latent nuclear-weapons potential".[42] Recently, scholars found yet another empirical proof of a focus on offensive cyber capabilities in the Defense Advanced Research Projects Agency (DARPA) so-called "Plan X", which, by building a user-friendly visualisation of cyberspace, is said to make it easier to conduct aggressive cyber operations.[43] In addition, activists long have been pointing out the fact that the US allegedly more often than not decides not to disclose so-called zero-days vulnerabilities,[44] keeping them for itself in order to achieve a strategic advantage over its adversaries, both in defence and offence.[45] Finally, despite such empirical proofs, it must be pointed out that a brilliant study conducted by Valeriano and Maness showed that the US vis-à-vis China malicious cyber activity constantly showed self-restraint, avoiding aggressive hard power responses, and preferring more traditional diplomatic ones.[46] Indeed, no such thing as a Stuxnet 2.0 materialised yet,

---

[42] Ivanka Barzashka, "Are Cyber-Weapons Effective?", *The RUSI Journal*, Vol. 158, No. 2 (2013), 48 - 56, 48.

[43] Noah Shachtman, "Darpa Looks to Make Cyberwar Routine with Secret 'Plan X'", *Wired*, August 21, 2012 (accessed June 2018), https://www.wired.com/2012/08/plan-x/; Noah Shachtman, "'Degrade, Disrupt, Deceive': U.S. Talks Openly About Hacking Foes", *Wired*, August 28, 2012 (accessed June 2018), https://www.wired.com/2012/08/degrade-disrupt-deceive/.

[44] Such a term refers to those vulnerabilities (within software and hardware) that have not been widely acknowledged by security service providers. They are truly valuable to attackers, which can exploit them to carry out attacks that can not initially be detected. Singer and Friedman, *Cybersecurity and Cyberwar,* 299.

[45] Tim Stevens, "Cyberweapons: Power and the Governance of the Invisible" (Forthcoming); Nicholas Weaver, "Is the NSA Doing More Harm Than Good in Not Disclosing Exploits?", *Foreign Policy*, September 25, 2017 (accessed June 2018), https://foreignpolicy.com/2017/09/25/is-the-nsa-doing-more-harm-than-good-in-not-disclosing-exploits-zero-days/.

[46] Valeriano and Maness, *Cyber War versus Cyber Realities.*

with the current "militarization" historical phase being one of cyber-skirmishes,[47] rather than devastating "cyber wars".

2.3. Analyses of official documents also utilised in the present thesis

Finally, important is to clarify how the literature has approached some of the official documents the present thesis also takes into account, which have been published since the early 2000s, therefore during the George W. Bush and Barack Obama presidencies. Overall, such documents have been analysed adopting specific theoretical lenses, or in a more straightforward fashion, putting them in relation with previous ones, but without venturing in IR and security studies theories.

Stevens carries out an analysis of some specific key official texts published under the Presidency of Barack Obama to demonstrate that there has been a shift towards a normative approach to cybersecurity and deterrence in cyberspace. In his brilliant and complex piece, Stevens looks at deterrence and at the constructivist understanding of norms, fusing the two to arrive at a paradigm that sees a degree of deterrence achieved through regulative norms, which are said to enhance the predictability of international actors. Precisely this is what seems to be driving the 2011 International Strategy for Cyberspace, namely a tendency to push for the agreement of regulative norms for cyberspace in following the role of a norm entrepreneur, which underlines the importance of cooperation and voluntary action. Of course,

[47] David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a strategy for cyber-power* (Adelphi series Book 424; The International Institute for Strategic Studies - IISS; Routledge; 1st edition, January 28, 2012) [Kindle Edition], Kindle Location 2363.

Stevens points out that achieving a regulatory and negotiated treaty for cyberspace is not something easy, given the various opposite interests at play, especially between the US and Russia, and accordingly he concludes by stating that one possibility is the achievement of norms of acceptable use rather that of non-use, thus something not even close to the taboo that developed regarding nuclear weapons.[48]

Mazanec's work finds a link with that of Stevens. Mazanec analysing the possibility of the emergence of norms for cyberspace adopting a refined norms life cycle theoretical framework, a central one within the constructivist literature, focuses on official US cyberspace strategies (partly the same as those in Stevens' article) to highlight what the US interests are regarding cyberspace capabilities and power. He argues that due to the perceived interests transpiring from the documents, official statements, and other empirical evidence, it does seem that the emergence of constraining norms is not in the US interest, a conclusion similar to what hinted by Stevens.[49] Precisely because on the emergence of so-called "cyber norms" a vast literature exists,[50] ranging from more critical to simply descriptive

---

[48] Tim Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace", *Contemporary Security Policy*, Vol. 33, No. 1 (April, 2012). 148 - 170.
[49] Brian M. Mazanec, *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons* (Potomac Books, November 1, 2015), Chapter 6.
[50] Besides the works of Stevens and Mazanec, see also: Tim Maurer, *Cyber norm emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber-security* (Discussion Paper #2011-11 Explorations in Cyber International Relations Discussion Paper Series Belfer Center for Science and International Affairs, 2011); Roger Hurwitz, "A New Normal? The Cultivation of Global Norms as Part of a Cybersecurity Strategy", in *Conflict and Cooperation in Cyberspace The Challenge to National Security*, edited by Panayotis A.

articles, and the argument presented in the present thesis standing also without directly engaging with it, such a specific topic has been left out of the analysis.

Chen also focuses on key official US documents concerning cyberspace and cybersecurity, some of which are the same also covered by Stevens and Mazanec. Chen's work is compelling because, despite not approaching such primary sources through a theoretical framework, it offers a rather rich picture on the evolution putting each strategy vis-à-vis its preceding ones. Already from the start, Chen highlights how some specific key themes repeat themselves across various official strategies, namely "a need for public-private sector cooperation, reduction of vulnerabilities, more cyber security training, and international cooperation",[51] and part of his analysis indeed seeks to highlight those themes that the 2011 DOD's Strategy for Operating in Cyberspace reprises from previous strategies. In total Chen's analysis focuses on the following documents, most of which also form part of the set of primary sources chosen in the present dissertation: the 2003 National Strategy to Secure Cyberspace; the 2004 Joint Chiefs of Staff's National Military Strategy of the United States of America; the 2006 Joint Chiefs of Staff's National Military Strategy for Cyberspace Operations (NMS-CO); the 2008 Comprehensive National Cybersecurity Initiative

---

Yannakogeorgos and Adam B. Lowther (Taylor & Francis, 2014), 233 - 264; Emilio Iasiello, "What Happens If Cyber Norms Are Agreed To?", *Georgetown Journal of International Affairs*, Vol. 17, No. 3 (Fall/Winter, 2016), 30 - 37.

[51] Thomas M. Chen, *An assessment of the Department of Defense Strategy for Operating in Cyberspace* - The Letort Papers (Strategic Studies Institute and U.S. Army War College Press, 2013), 2.

(CNCI); the 2011 International Strategy for Cyberspace; and finally of course the 2011 DOD's Strategy for Operating in Cyberspace. Chen analysis of the 2011 DOD's strategy concludes that through such document the US clearly signalled some specific messages. Firstly, that DOD will maintain superiority in cyberspace, and secondly, that cooperation with the private sector and allies and like-minded states is crucial. Overall, Chen argues that such strategy falls short under several aspects since it is "not clear about priorities, futuristic vision, progress metrics, or enforcement and accountability".[52]

Barnard-Wills and Ashenden, studying the cyber-discourse adopting the "govermentality" theory derived from Foucault, analyse one key document published by the Obama Administration in 2009, the so-called Cyberspace Policy Review. Not directly taken into account in the present dissertation, such a document highlights the importance cybersecurity reached during the Obama presidency, stressing the importance to reach specific defensive capabilities, as well as "encouraging research, development, and training in cyber security".[53]

Overall, of most importance for the present dissertation is the work of Saltzman who, adopting a redefined Offense-Defense balance theory to accommodate cyberspace showing the prominence of offense over defence, analyses the US cyber strategic posture. Through an analysis of key officials documents between 2003 and 2011 (mostly the same as the already

[52] Ibid., 36.
[53] Barnard-Wills and Ashenden, "Securing Virtual Space", 113.

mentioned works), Saltzman argues that the US seems to be showing a strategic posture characterised by a "paradoxically defensive nature", or in other words by a general defensive tone constellated by some ambiguity and occasional hints of offensive reasoning.[54] Regarding the US, Saltzman concludes by saying that "[t]he intellectual evolutionary process pursued by officials in the military and civil branches of government is still ongoing, and the United States is far from having a comprehensive cyber strategy".[55]

Finally, regarding US official strategies, recently scholars have focused on the latest DOD's Cyber Strategy. Fore example, Myauo in her analysis of such DOD's strategy also touches upon some other regulations and official documents published by the US federal government and White House, focusing especially on critical infrastructure protection. Her analysis mainly deals with the DOD's strategy's call to partnerships between CYBERCOM and governments, academia, and industry. From a rather non-theoretical approach, Myauo focuses on the possibilities partnerships between the military and other civil institutions, for example on the so-called IT portfolio and predictive analytics, could have in enhancing the "overall resiliency of U.S. networks and systems".[56]

2.4. Is it possible to speak of a gap? - main take away from the literature

[54] Saltzman, "Cyber Posturing and the Offense-Defense Balance".
[55] Ibid., 56.
[56] Michele Myauo, "The U.S. Department of Defense Cyber Strategy: A Call to Action for Partnership", *Georgetown Journal of International Affairs*, Vol. 17, No. 3, (Fall/Winter, 2016), 21 - 29, 27.

This literature review has shown that already much has been written on topics of interest for the present thesis. Indeed, the author believes that speaking of a gap, as in an entirely blank spot within the literature, might not be entirely correct. The arguments, insights, and context transpiring from the mentioned literature entries need to be understood as vines onto which the thesis latches; indeed, for the sake of its own dissertation the author owns very much to them.

As shown, various scholars approached the discourse from a rather critical point of view, highlighting how the processes of social construction of threats have been utilised to justify specific actions and policies. Further, in analysing the "militarization" historical moment, scholars already have provided some insights regarding the US starting to go offensive within the cyber domain, clarifying however that a degree of restraint and a focus on norm promotion seem to be guiding such a country's approach to cybersecurity, with a holistic and complete strategy missing. Finally, analyses of official documents dealings precisely with the cyber medium and threats spawning from it have been produced.

Despite all that, some room does exist for pushing the knowledge a bit forward. The works of both Saltzman and Chen, which take into account many official documents, juxtaposing them to better understand the evolution of US strategic thinking, can be further extended implementing new documents released posthumous of such two scholarly works. For instance, the "paradoxical defensive nature" thesis brought forward by Saltzman can be tested on such new empirical material. In addition,

whether most of the articles focusing on the analysis of discourse state their theoretical and methodological groundings, the majority of those addressing key US official documents fail to address the specific kind of methodology implemented. Arguably, since they all deal with written primary sources, they all adopt some form of discourse analysis, still this lack of methodological rigour calls for more methodological-driven analyses.

However most of all, what truly seems to be missing is an initial analysis that studies the US approach to cyberspace from a more ideational point of view. Indeed, to the author's knowledge, the conceptualisation adopted in this work still has not been presented within the literature. For instance, this somewhat gap is precisely the one the present thesis seeks to "close". Scholars already appreciated the fact that during the "militarization" phase states have moved onto more offensive postures regarding the adoption of cyber-related technologies and medium itself. The present thesis starts from such a context and empirical argumentations, approaching such an analysis from a rather different theoretical and methodological perspective. As better explained in the upcoming chapters, despite the adoption of a discourse analysis, focus is posed on themes and on the role norms have in informing an actor's approach to a technology and medium. In other words, by grounding a thematic-discourse analysis within Constructivism and strategic culture, the present thesis' humble contribution is that of producing new knowledge on whether it is possible to appreciate a "shift" within the US "cyber strategic culture", taking as empirical proofs

especially the concept of “active cyber defence" (ACD) measures, the 2015 DOD’s Cyber Strategy, and the 2017 National Security Strategy (NSS).

3. Theoretical background of the thesis

The present chapter outlines the theoretical background of the thesis, or in other words the theories from which it draws inspirations and insights. Overall, key tenets of Constructivism and Strategic Culture research tradition do form the theoretical ground onto which the dissertation latches, especially regarding the power norms have to shape/inform political and strategic behaviour, hence culture. The present chapter firstly introduces some key characteristics of such two research and theoretical traditions, then concluding with a description of the framework followed in the present composition.

3.1. Constructivism

Onuf firstly introduced the term Constructivism at the end of the 1980s.[57] As one key meta-theoretical approach to the study of IR and security, Constructivism saw the light mirroring a sense of dissatisfaction felt by scholars towards more classical IR theories, which were deemed unfit to thoroughly explain some key specific historical moments that happened since the end of the Cold War.[58] The starting point of Constructivism is indeed a critique of the rationalist and materialist assumptions at the bottom of both realism and liberalism. Rather than understanding actors as

[57] Nicolas Onuf, *World of Our Making: Rules and Rule in Social Theory and International Relations* (Routledge, 2012).
[58] Robert Jackson and Georg Sørensen, *Introduction to International Relations: Theories and Approaches* (Oxford University Press, 4th edition, April 19, 2010), 162.

utility-maximising ones, constructivists conceive them as social ones, stressing the importance of non-material milieus,[59] "such as ideas, norms, knowledge, [and] culture".[60] Point of departure for constructivists is indeed the conception that meaning is "socially constructed".[61] In opposition to the individualist ontology characterising rationalist approaches, constructivists are entrenched in a social ontology, which asserts that actors (domestic and international) "cannot be separated from a context of normative meaning which shapes who they are and the possibilities available to them".[62] For instance, the international system itself is not something given, but rather something that "exists only as an intersubjective awareness among people, constituted by *ideas*, [rather than only] material forces".[63] Scholars of such a school of thought are interested in uncovering how a particular meaning is achieved, and how this then influence/informs politics. In other words, constructivists seek to give better explanations and analyses on how both material and ideational factors speak to each other in providing various possibilities and outcomes of political action.[64] Accordingly, the analysed process of constitution is understood as causal, "since how things are put

[59] Mike Bourne, *Understanding Security* (Palgrave, 2014 edition), 51.
[60] Martha Finnemore and Kathryn Sikkink, "TAKING STOCK: The Constructivist Research Program in International Relations and Comparative Politic", *Annual Review of Political Science*, Vol. 4 (June, 2001), 391 - 416, 392.
[61] Ian Hurd, "Constructivism", in *The Oxford Handbook of International Relations*, edited by Christian Reus-Smit and Duncan Snidal (Oxford University Press Inc., 2010), 298 - 316, 300.
[62] Tim Dunne, Milja Kurki, and Steve Smith, *International Relations Theories* (Oxford University, 2013), 190.
[63] Jackson and Sørensen, *Introduction to International Relations*,162. Emphasis in the original.
[64] Dunne, Kurki, and Smith, *International Relations Theories*, 189.

together makes possible, or even probable, certain kinds of political behaviour and effect".[65]

Wendt, a key figure within such meta-theoretical approach, argues that "anarchy is what states make of it",[66] underlying that international actors seek security by interpreting both capabilities and intentions of their counterparts. In doing so, they are guided by their own identities, specific values, and types of behaviour seen as natural or desirable, which are not given, but produced and re-produced precisely during such process of interpretation. [67] Therefore, for constructivists the entire international system is socially constituted, built on ideational factors rather than material ones, open to change and evolution. Overall, the actions of states not only shape the arena in which they exist, but while doing so their own identities and interests are formed as well. This is the logic of co-constitution, or in other words the "logic of appropriateness", which drives the constructivism understanding of the relationship existing between structures and agents.[68]

When studying such a process, many constructivists have focused their attention on "norms", independent variables either international or

---

[65] Finnemore and Sikkink, "TAKING STOCK", 394.
[66] Alexander Wendt, "Anarchy is what States Make of it: The Social Construction of Power Politics", *International Organization*, Vol. 46, No. 2 (Spring, 1992), 391 - 425.
[67] Bourne, *Understanding Security,* 51; Wendt, "Anarchy is what States Make of it", 392; Jackson and Sørensen, *Introduction to International Relations*, 168.
[68] Dunne, Kurki, and Smith, *International Relations Theories*, 190; Hurd, "Constructivism", 304.

domestic "that can influence international behaviour",[69] shaping "realms of possibility".[70] Norms have been conceptualised in various similar ways, with a rather accepted and utilised one found in Katzenstein who understands them as "collective expectations about proper behaviour of actors for a given identity",[71] therefore "prescriptions or proscriptions for behaviour".[72] Moreover, it must be understood that norms do not necessarily determine outcomes, but rather constitute or create what have been called "realms of possibility.[73] For the sake of the analysis carried out in the present thesis, the definition offered by Farrell is taken as most valid. He conceptualises norms as "intersubjective beliefs about the social and natural world that define actors, their situations, and the possibilities of action[, which are] reproduced through social practice".[74] Different kind of norms are said to exist according to their effects; whether regulative ones constrain already existing activities; constitutive ones define "the set of practices that make up any particular consciously organized social activity [specifying] what counts as that activity".[75] Or, as Finnemore and Sikkink

---

[69] Mazanec, *The Evolution of Cyber War: International Norm for Emerging-Technology Weapons*, Chapter 1.
[70] Nina Tannenwald, "The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use", *International Organization*, Vol. 53, No. 3 (Summer, 1999), 433 - 468, 435.
[71] Ronald L. Jepperson, Alexander Wendt, and Peter J. Katzenstein, "Norms, Identity, and Culture in National Security", in *The Culture of National Security: Norms and Identity in World Politics*, edited by Peter J. Katzenstein (New York: Columbia University Press, 1996), 33 - 75, 34.
[72] Tannenwald, "The Nuclear Taboo", 436.
[73] Ibid., 435.
[74] Theo Farrell, "Constructivist Security Studies: Portrait of a Research Program", *International Studies Review,* Vol. 4, No. 1 (Spring, 2002), 49 - 72, 49.
[75] John Gerard Ruggie, *Constructing the World Polity* (New York: Routledge, 1998), 22.

put it, "regulative norms […] order and constrain behavior, [while] constitutive norms […] create new actors, interests, or categories of action".[76] Constructivists are mainly interested in the second ones, since in following the logic of appropriateness they argue that norms go "all the way down", creating and defining actors' identities and interests,[77] as well as the rules and practices deemed acceptable on the international stage.[78] The fact that norms precede international actors' interest is what distinguishes Constructivism from other approaches.

Within the field of security studies, seminal works grouped within the famous edited volume *The Culture of National Security,* all demonstrate the role various social structures play in reshaping "actor's interests, self-understanding, and behavior", [79] highlighting therefore that "security interests are defined by actors who respond to cultural factors",[80] or in other words, the causal effects norms do have within state actors.

3.2. Strategic culture

[76] Martha Finnemore and Kathryn Sikkin, International Norm Dynamics and Political Change, *International Organization*, Vol. 52, No. 4 (Autumn, 1998), 887 - 917, 891.
[77] Stevens, "A Cyberwar of Ideas?", 155.
[78] Farrell, "Constructivist Security Studies", 52.
[79] Finnemore and Sikkink, "TAKING STOCK", 396.
[80] Peter J. Katzenstein, "Introduction: Alternative Perspectives on National Security", in *The Culture of National Security: Norms and Identity in World Politics*, edited by Peter J. Katzenstein (New York: Columbia University Press, 1996), 1 - 32, 2.

The focus on ideational factors, such as culture and norms indeed, arguably constitutes the bridge linking Constructivism to studies of strategic culture. In fact, during the 1990, constructivists somewhat gave new nourishment to a research agenda that had fallen in disarray after the end of the Cold War. Further, as clarified by Hurd, focusing on norms does not regardlessly exclude the possibility to approach also the study of strategic behaviour, indeed many constructivists approach power and interest similarly to realists, agreeing that international actors behave in pursing perceived interests, as well as arguing that separating the study of the logic of consequence from that of the logic of appropriateness is a mistake.[81]

The study of strategic culture within the broader security studies literature can be traced back to Snyder's seminal work on Soviet and American nuclear doctrine, published in 1977 by the Rand corporation.[82] After a drawback right at the end of the Cold War, especially during the 1990s, and somewhat recently, such field of study got reinvigorated, being applied to a variety of case studies, moving away from the exclusive focus on nuclear weapons. Overall, scholars adopting the concept of strategic culture have been interested in analysing and building frameworks through which explain the strategic behaviours adopted by international actors vis-à-vis their peculiar strategic properties.[83] Further, through the application of

---

[81] Hurd, "Constructivism", 310.

[82] Jack Snyder, *The Soviet Strategic Culture: Implications for Limited Nuclear Operations* (Santa Monica: RAND, 1977).

[83] Edward Lock, "Strategic Culture Theory: What, Why, and How", *Oxford Research Encyclopedia of Politics,* September 26, 2017 (accessed May 2018),

such concept, scholars seek to understand and explain continuity and change within the chosen case studies' national security policies. Within the literature it is often pointed out that the term strategic culture, despite being constantly used, still remains surrounded by a high degree of confusion, with many definitions and approaches to it currently existing.[84] Indeed, three key schools or "generations" exist, each differing on specific epistemological premises,[85] with a fierce on-going debate especially between two of such "generations", the first and third one, respectively lead by Gray and Johnston.

In general terms, strategic culture can be defined as "the set of beliefs, assumptions, attitudes, norms, world views and patterns of habitual behaviour held by strategic decision-makers regarding the political objectives of war, and the best way to achieve it".[86] In line with this view, Johnston understands the concept of strategic culture as "an ideational milieu which limits behavioral choices";[87] an independent variable that helps explaining behaviour. Johnston's approach is strongly grounded in a positivist philosophical position finding a link with Popper's falsification theory. From such premises, Johnston indeed argues that "theories positing

---

http://politics.oxfordre.com/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-320.

[84] Ibid.

[85] Edward Lock, "Refining strategic culture: Return of the second generation", *Review of International Studies*, Vol, 36, No. 3 (2010), 685 - 708.

[86] Yithzak Klein, "A theory of strategic culture", *Comparative Strategy*, Vol. 10, No. 1 (1991), 3 - 23, 3; Alessia Biava, Margriet Drent, and Graeme Herd, "Characterizing the European Union's Strategic Culture: An Analytical Framework", *Journal of Common Market Studies*, Vol. 49, No. 6 (2011), 1227 - 1248, 1228.

[87] Alastair Iain Johnston, *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History* (Princeton: Princeton University Press, 1995), 46.

the influence of strategic culture on actions should be 'falsifiable', or at least distinguishable from non-strategic culture variables". [88] Contrary to Johnston, Gray contends that strategic culture "comprises the persisting (but not eternal) socially transmitted ideas, attitudes, traditions and habits of mind and preferred methods of operation [so, behavioural patterns] that are more or less specific to a particular geographically based security community that has had a necessarily unique historical experience". [89] Therefore, culture needs to be understood as "context",[90] as something that "goes all the way down" in comprising and pervading political actors' behaviour. [91] According to this view, it is wrong to artificially detach culture from behaviour, hence that studying strategic culture through the adoption of positivist methods of social science is not possible.[92] Whether Johnston appears to approach culture as an independent causal variable useful to analyse and predict change in strategic choices, Gray sees culture as a context, which helps scholars understanding both reasons and motivations lying at the base of actors' actions. [93] This is precisely the Johnston-Gray debate, an on-going intellectual competition on whether the concept of strategic culture determines or rather shapes strategic

---

[88] Christoph O. Meyer, "Convergence Towards a European Strategic Culture? A Constructivist Framework for Explaining Changing Norms", *European Journal of International Relations*, Vol. 11, No. 4 (2005), 523 - 549, 527.
[89] Colin Gray, "Strategic Culture as Context: The First Generation of Theory Strikes Back", *Review of International Studies*, Vol. 25, No. 1 (1999), 49 - 69, 51; Alan Bloomfield, "Time to Move On: Reconceptualizing the Strategic Culture Debate", *Contemporary Security Policy*, Vol. 33, No. 3 (2012), 437 - 461, 445.
[90] Gray, "Strategic Culture as Context", 51.
[91] Meyer, "Convergence Towards a European Strategic Culture?, 527; Gray, "Strategic Culture as Context".
[92] Lock, "Refining strategic culture: Return of the second generation", 690.
[93] Meyer, "Convergence Towards a European Strategic Culture?, 527.

decision-making.

3.3. Theoretical insights driving the present research agenda

Precisely an agenda rooted in the study of strategic culture, with insights also from Constructivism, is what the present thesis is seeking to follow when analysing the US approach to (national) cybersecurity. Following such an agenda is important and pertinent since it usually asks one key question also asked in the present thesis, namely "What are the ideational foundations of national security policy?".[94] As already mentioned, the author introduces and utilises the term "cyber strategic culture". Such a term indicates the ideational milieu constituted of and informed/mirrored by symbols, ideas, and ultimately norms,[95] displaying the strategic behaviours deemed best to be adopted on matters linked to national cybersecurity. Overall, the conceptualisation of strategic culture given by Meyer is deemed best for the present thesis, "the socially transmitted, identity-derived norms, ideas and patterns of behaviour that are shared among a broad majority of actors and social groups within a given security community, which help to shape a ranked set of options for a community's pursuit of security and defence goals".[96] Here lies the cautious-Constructivist approach of the present work, namely the study on those

---

[94] Jeffrey S. Lantis, "Strategic Culture: From Clausewitz to Constructivism", in *Strategic Culture and Weapons of Mass Destruction: Culturally Based Insights Into Comparative National Security Policymaking*, edited by Jeannie L. Johnson, Kerry M. Kartchner, and Jeffrey A. Larsen (Palgrave Macmillan, 2009), 33 - 54, 33.
[95] Toby Lauterbach, ""Constructivism, Strategic Culture, and the Iraq War", *ASPJ Africa & Francophonie*, Vol. 2, No. 4 (4th Quarter, 2011), 61 - 92, 62.
[96] Meyer, "Convergence Towards a European Strategic Culture?", 528.

ideational structures that participate in informing and mirroring actors' strategic choices and behaviours. The approach is in line with conventional constructivism, since the aim of the present work is not fully critical,[97] and also cautious since no claims of causality are directly made, with the debate on the logic of appropriateness and consequences also left aside. Moreover, the present thesis does not engage with international norms, but rather extrapolates those that seem to be guiding the US by analysing its "cyber strategic culture", which transpires from the assessed primary sources. Finally, whether traditional strategic culture studies have mainly analysed behaviours regarding the use or non use of military force, the present thesis expands such a focus also on strategic choices not directly involving the use of force, as better outlined further down.

The following chapter further explains from a technical-methodological point of view how such research program is achieved, focusing mainly on the role and interpretation of discourse and primary data utilised.

[97] Reus-Smit argues that Constructivism is split in two camps; between those who remain attached to its critical origins and those who have embraced it as simply an "explanatory or interpretive tool". Christian Reus-Smit,"Constructivism", in *Theories of International Relations*, edited by Scott Burchill et al. (Palgrave Macmillan, 3rd edition, 2005), 188 - 212, 204.

4. Methodology adopted to deliver the stated thesis' goal

The present chapter aims at outlining the kind of practical methodology utilised in the present thesis to reach its goal. In building a bridge with the mentioned constructivism meta-theoretical approach, a methodology grounded in the qualitative research tradition centred on the analysis of discourse and themes has been chosen. Besides explaining the characteristics and reasons of such a methodology, the present chapter also offers elucidations regarding the selected case study, the primary sources utilised, and the overall limitations of the dissertation itself.

Having a section delineating the methodology utilised is rather important since it helps achieving a certain degree of transparency, which is key in every academic type of work.

The present chapter proceeds as following: firstly, the case study selected is covered; secondly, information regarding the data corpus is given; thirdly, focus is posed on the discourse-thematic approach; and lastly, the limitations of the dissertation are discussed.

4.1. Case selection

The present dissertation focuses on one specific international actor, namely the United States of America. Such a choice was dictated by several reasons. Within the international arena many other states figure as prominent regarding cyber-related issues, and indeed scholars also placed their

academic lenses over countries such as Russia,[98] China,[99] Japan,[100] Germany, France, and the United Kingdom,[101] as well as on minor ones, such as the Baltic and Visegrád Group ones.[102] All of these in fact have recently been started publishing official documents and strategies that deal with cybersecurity and cyber-related issues, providing scholars with more primary data to work with.

Nevertheless, the choice has fallen on the US mainly because of its prominent role in the "cyber-international arena", hence in discussions linked to cybersecurity, cyber warfare, cyber power etc., in various international fora, and especially at the UN.

Moreover, the US as a country is one of the ones that most relies on such a man-made domain, with its society being highly digitalised, both at the private and public level, something that places it in a peculiar position regarding its overall cybersecurity and cyber power, therefore a truly interesting case from an analytical point of view. Indeed, given its historical link to the creation of the Internet, the debate regarding its usage and governance, and its overall importance for the wellbeing and prosperity of the country, made the US one of the first ones to publish specific official

---

[98] Mazanec, *The Evolution of Cyber War*, Chapter 5.

[99] Francis C. Domingo, "China's Engagement in Cyberspace", *Journal of Asian Security*, Vol. 3, No. 2 (2016), 245 - 259.

[100] Paul Kallender & Christopher W. Hughes, "Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace", *Journal of Strategic Studies*, Vol. 40, No. 1-2 (2017), 118 - 145.

[101] Agnija Tumkevič, "Uncertain Security Community: Building Western Cybersecurity Order", in *ECCWS 2017 16th European Conference on Cyber Warfare and Security*, edited by Mark Scanlon and Neihn-An Le-Khac (ACPIL, June 12, 2017), 497 - 505.

[102] Tumkevič, "Cybersecurity in Central Eastern Europe".

documents dealing with the cyber medium, being nowadays the richest international actor in terms of the quantity of such documents publicly available. According to some experts, the US "has been in the vanguard of developing cyber security policy and strategy",[103] also being the main "sender of ideas" regarding IT problems and solutions.[104]

Finally, on a more personal level, the choice was guided by the author's language competencies. Given that the US is an English speaking country, the assessed primary documents are all written in such a language, as opposite to other countries that might publish in English only reduced versions of their official documents, something that would limit the overall research.[105]

4.2. Gathered and utilised data sources

Regarding the data utilised for the present thesis, it has been extracted from both primary and secondary sources. Whether the gathered primary sources have been utilised to conduct the further discussed thematic analysis, the secondary ones have provided valuable data through which

[103] Piret Pernik et al., National Cyber Security Organisation: United States (Tallinn, NATO CCD COE, 2016). Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf, 7.

[104] Cavelty Dunn, *Cyber-Security and Threat Politics*, 9.

[105] The fact that documents might be published in an abridged format is a possibility always present, therefore exclusive of translated versions. For instance, some specific official documents might have an official "internal" version distributed within governmental organisations, and a shorter version published for the wider public.

further push the thesis' overall argument(s), and draw more insights especially on the concept of "active cyber deference" (ACD) measures.

Regarding the primary sources, the author has gathered and analysed key official security and military strategies published by both the White House and the Military apparatus since the early 2000s, which either partially or completely deal with cyberspace, cybersecurity, and cyber warfare -related matters. Therefore, the sources utilised are all of textual nature. The reason why focus has been posed to such kind of documents is easily discernible and closely linked to the thesis overall goals. As discussed in previous sections, the present dissertation aims at analysing the evolution of the US strategic thinking regarding cyberspace, or in other words grasp the evolution of what has been called the US "cyber strategic culture". Arguably, to acknowledge the strategic thinking of a country, or its strategic culture, the researcher should focus on security strategies, which despite not being politically nor legally binding in nature, can be regarded as frameworks guiding a state external and internal actions vis-à-vis a wide range of threats, also containing the means and conditions to fulfil certain purposes.[106] For instance, Lauterbach, to trace the US strategic culture and a possible shift of it within the context of the Iraq War, as primary sources

[106] Julia Klohs and Arne Niemann, "Comparing the US National Security Strategy and the European Security Strategy in the first decade of the 21st century: converging but still different", *Mainz Papers on International and European Politics (MPIEP),* No. 8 (2014), 2; Asle Toje, "The EU Security Strategy Revised: Europe Hedging Its Bets", *European Foreign Affairs Review*, Vol. 15, No. 2 (May, 2010), 171 - 190, 177.

utilises strategies and doctrines.[107] Moreover, (if possible) focus should be posed also on transcripts of decision-making processes, participants' memoirs, and elite interviews, as they allow to dive deeper within the mechanisms at work at the strategic level of a country.

The primary documents making up the data corpus have been retrieved online; downloaded either directly from the White House and Department of Defense,[108] or from related and third-party websites. In total, twelve official texts have been utilised within the research.[109] Such number might not seem large enough, however at this point in history not many more similar documents seem to be available. Further, during the research process the author came to the conclusion that implementing more primary sources would have failed in adding value to the analysis, not really altering nor challenging the obtained results. For instance, as an example, documents produced by the Department of Homeland Security (DHS) have been left out. Nonetheless, for the sake of transparency some other primary documents that have not been directly taken into account are briefly pointed out in an upcoming chapter. Moreover, it must be said that among

[107] Lauterbach, "Constructivism, Strategic Culture, and the Iraq War"
[108] The websites are the following: www.whitehouse.gov and www.defense.gov.
[109] In chronological order, the primary documents are the following: The National Strategy to Secure Cyberspace; The National Military Strategy of the United States of America 2004; The National Military Strategy for Cyberspace Operations; the National Security Strategy 2010; The National Military Strategy of the United States of America 2011; the International Strategy for Operating in Cyberspace. Prosperity, Security, and Openness in a Networked World; The Department of Defense Strategy for Operating in Cyberspace; Presidential Policy Directive No. 20; the National Security Strategy 2015; The DOD Cyber Strategy*;* The National Military Strategy of the United States of America 2015; and the National Security Strategy 2017.

all the selected primary sources two were secretive in nature. The first one is the 2006 National Military Strategy for Cyberspace Operations and the second one is the Presidential Policy Directive No. 20 (PPD-20). The first one was officially declassified under the "Freedom of Information Act" (FOIA), while the second one, despite not being officially made available to the wider public opinion, was publicly disclosed and shared by the whistle-blower Edward Snowden during his campaign of leaks.[110] The author is conscious that utilising secretive documents might go against academic standards and rules; however, if the 2006 document has been officially unclassified, PPD-20 has already been empirically used by academics,[111] being also rather important for the analysis conducted in the present dissertation.

Finally, to the reader it might seem that the actual analysis only is carried out on some documents, since some specific ones stand out, with sub-chapters entirely dedicated to them. However, the chosen methodology has been applied to all primary sources, with the majority of them having been grouped together.

As for the secondary sources, several main types of documents have been assessed and gathered. For instance, from the academic world, books and articles published by prominent journals and publishing houses have been gathered, with pieces of information extrapolated from them. The same has been done for news articles published on various online newspapers, as

---

[110] BBC, "Edward Snowden: Timeline", *BBC*, 20 August, 2013 (accessed May 2018), http://www.bbc.com/news/world-us-canada-23768248.

[111] See for example: Jeffrey Carr, "The Misunderstood Acronym: Why Cyber Weapons Aren't WMD", *Bulletin of the Atomic Scientists*, Vol. 69, No. 5 (2013), 32 – 37.

well as from some documents containing policy recommendations published by either think thanks. Articles published in academic journals have been mainly retrieved through the online portals of the Glasgow and Charles universities' libraries. Specific keywords linked to the thesis main topics have been utilised to speed up the research process, with some key journals being directly assessed through their own websites. In addition, books have been either directly downloaded from the Internet or accessed on digital reading application, or physically consulted at such two universities' libraries. As for news and think thanks' articles, they have been retrieved and downloaded online through searches made utilising the Google search engine.

4.3. Qualitative research tradition

With the word "quality" referring "to the what, how, when, and where of a thing […], [q]ualitative research [appears to be closely linked to] the meanings, concepts, definitions, characteristics, metaphors, symbols, and descriptions of things".[112] Not surprisingly, in a rather straightforward and common sense way, qualitative methods have been defined as "data collection and analysis strategies that rely upon the collection of, and analysis of, non-numeric data".[113]

---

[112] Bruce L. Berg, *Qualitative Research for the Social Sciences* (Pearson, 4th edition, 2001), 3.
[113] Christopher Lamont, *Research Methods in International Relations* (SAGE Publications Ltd, 1st edition, May 20, 2015) [Kindle Edition], 77.

Given the present thesis' focus on the analysis and interpretation of a rather contained set of written textual primary sources, it makes sense to methodologically ground it within the tradition of qualitative research, which in the field of IR studies, according to some, is the predominant one,[114] also from a "technical" point of view.

4.4. Discourse analysis

Central to the overall methodology adopted within the dissertation is the role played by discourse and its analysis. Discourse analysis is a vast field encompassing several methods, which are grounded in as many theories and philosophies, especially Constructivism, as seen in the literature review. Also in the present thesis the study of discourse is linked to such IR and security studies school of thought.

The Merriam-Webster online dictionary defines discourse, among others, as "a mode of organizing knowledge, ideas, or experience that is rooted in language and its concrete contexts (such as history or institutions)".[115] Similarly, the thesis understands discourse as a vehicle capable of shaping actors' "boundaries of the possible",[116] which "guide[s] political action[s] by denoting appropriate or plausible behaviour in light of an agreed

[114] Andrew Moravcsik, "Active Citation: A Precondition for Replicable Qualitative Research", *Political Science and Politics*, Vol. 43, No. 1 (January, 2010), 29 - 35.
[115] Merriam-Webster, n.d., "Discourse", *Merriam-Webster.com*, last updated May 12, 2018 (accessed May 2018), https://www.merriam-webster.com/dictionary/discourse.
[116] Klohs and Niemann, "Comparing the US National Security Strategy and the European Security Strategy in the first decade of the 21st century", 6.

environment".[117] Or better, as "structures of signification which construct social realities[,] make intelligible some ways of being in, and acting towards, the world [as well as pushing forward] a particular 'regime of truth' while excluding other possible modes of identity and action".[118]

National strategies are official texts, which do not have a political nor legal binding power. Nonetheless, since such documents are produced and published by governmental and other national bodies, they do signal the range of behaviours that form a state's conduct vis-à-vis states priorities and domestic, regional, and global context. Put simply, national strategies can be considered as guiding frameworks for actions, [119] sharing such possibilities through discourse.

It must be pointed out that due to their nature and drafting and revising processes such documents go through, they often are "semantically neutral", lacking in metaphors or other semantic constructions. Due to such a characteristic, adopting key techniques often used when conducting critical discourse analysis might not be feasible. Nevertheless, national strategies do contain specific discourses that might dominate over others. In this case, a student might look at what is missing, as in words or specific

[117] Ibid.

[118] Jennifer Milliken, "The Study of Discourse in International Relations: A Critique of Research and Methods", *European Journal of International Relations*, Vol. 5, No. 2 (1999), 225 - 254, 229.

[119] Klohs and Niemann, "Comparing the US National Security Strategy and the European Security Strategy in the first decade of the 21st century", 2.

expressions, rather than at what is present within a text, to uncover what kind of specific behaviour the discourse legitimates.[120]

Overall, the aim of the discourse analysis applied within the thesis is not critical, it does not aim at proving that certain power dynamics are being normalised or justified, precisely because the primary sources utilised do not really lend themselves to such an analysis. For instance, it does not seek to replicate some of the works cited within the literature review, which drawing from critical Constructivism explored the way cyber-related issues have been framed in specific ways to justify some specific actions and behaviours. Rather, it approaches discourse understanding it as a social structure, a milieu, through which norms informing a strategic culture travel. In other words, it conceptualises it as the vehicle through which recorded beliefs (norms) are shared, thus where physical traces of them can be grasped.[121]

Finally, whether "full-fledged" constructivists underline that language itself it socially constructed, pointing out that an "objective" basis through which identify material reality is lacking, the present thesis rejects such fully interpretative conceptualisation, embracing a more positivist stance towards discourse. Accordingly, in carrying out the analysis the idea that objects of enquiry "can exist independently of the analyst [and] consensus

[120] Gery W. Ryan and H. Russel Bernard, "Techniques to Identify Themes", *Field Methods*, Vol. 15, No. 1 (February, 2003), 85 - 109.
[121] Farrell, "Constructivist Security Studies", 60

about the nature of the world [being] possible in the long run" is followed.[122]

The aim is to extrapolate those words and passages that convey specific actions, then clustering them together under two specific "macro thematic categories" to achieve the mentioned thematic discourse methodology.

4.5. Thematic analysis

Already from its name, it is clear that thematic analysis deals with the discovery of themes, being indeed often described as "a method for identifying, analysing, and reporting patterns (themes) within data[, and which] minimally organises and describes [a] data set in (rich) detail".[123]

Within the literature, a veil of ambiguity seems to surround the concept of thematic analysis. Scholars have indeed pointed out that such a method "has been poorly [or not at all] branded",[124] and often understood as being part of more common and widely utilised qualitative methods of enquiry.[125] In other words, as a tool researchers can turn to when conducting their

[122] Cavelty Dunn, *Threat Politics*, 7
[123] Virginia Braun and Victoria Clarke, "Using thematic analysis in psychology", *Qualitative Research in Psychology*, Vol. 3, No. 2. (2006), 77 - 101, 79.
[124] Lorelli S. Nowell, et al., "Thematic Analysis: Striving to Meet the Trustworthiness Criteria", *International Journal of Qualitative Methods*, Vol. 16 (2017), 1 - 13, 1.
[125] Richard E. Boyatzis, *Transforming Qualitative Information: Thematic Analysis and Code Development* (SAGE Publications, Inc, 1st edition, April 16, 1998).

qualitative analyses,[126] rather than as a standalone technique to analyse data. Paradoxically, precisely due to such poor branding and extensive (unconscious) use, thematic analysis is said to "possibly [be] the most widely used qualitative method of data analysis".[127]

Despite such branding issue, scholars have argued that thematic analysis deserves to be under the spotlight within the qualitative research tradition since it provides researchers with skills useful to then conduct other more complex qualitative enquiries.[128]

Thematic analysis fits the present dissertation for many reasons. One is its flexibility and theoretical freedom. Within the literature it has been pointed out that thematic analysis is truly valuable to those researchers who still are building experience on both theory and knowledge regarding qualitative approaches.[129] Further, given its flexibility, thematic analysis lends itself to a wide application across many fields and, most of all, to various epistemologies. Secondly, since the present work does not utilise a too broad set of primary sources, nor the data extrapolated from them is too vast, thematic analysis has been chosen for the present research since it is

---

[126] Christian Herzog, Christian Handke, and Erik Hitters, "Thematical Analysis of Policy Data", in T*he Palgrave Handbook of Methods for Media Policy Research*, edited by Van den Bulck, H, Puppis, M., Donders, K. & Van Audenhove, L (Basingstoke: Palgrave Macmillan, forthcoming), chapter 8. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3068081.

[127] Virginia Braun and Victoria Clarke, *Successful qualitative research: A practical guide for beginners* (SAGE Publications Ltd, 1st edition, April 5, 2013), 175.

[128] Braun and Clarke, "Using thematic analysis in psychology".

[129] Nowell, et al. "Thematic Analysis", 2.

said to be applicable to both small and medium-sized sets of data.[130] Thirdly, it appears that thematic analysis is most useful when applied to an entire data set, rather than within single data items.[131] In other words, it works best when used to analyse recurrent patterns among a set of primary sources, rather than within one specific source, something in line with the aim of the present thesis. And finally, most important of all, thematic analysis has been chosen in the present dissertation since it offers researchers a rather clear structure to adopt when analysing the data that leads to the highlighting of themes. Given that the research intends to analyse two themes present within the US "cyber strategic culture" in order to evaluate whether an evolution took place since the early 2000s, thematic analysis does feel as one of the best techniques to adopt.

Traditionally, thematic analysis has been presented as a rather linear 6-step process, involving specific phases, each building on the preceding one, which in brief are the following: 1) familiarising with the data; 2) generating initial codes; 3) searching for themes; 4) reviewing themes; 5) defining and naming themes; 6) writing the report.[132]

Having clear and structured methodological framework is important since it helps conveying analytical clarity and trustworthiness, however as it often happens within the qualitative research tradition, such a path ends up being more tortuous, with researchers moving back and forth throughout it

[130] Braun and Clarke, *Successful qualitative research*, 50.
[131] Braun and Clarke, "Using thematic analysis in psychology", 81.
[132] Ibid.

in an iterative and reflective manner,[133] a situation that manifested itself also while working on the present dissertation. Moreover, in carrying out the analysis of the primary sources, such a rather strict and rigid framework has been revisited and modelled according to the characteristics of the utilised primary sources and data, as well as to accommodate the thesis' needs. As further explained, some passages have been revisited and cut.

Coding involves "taking text data […] gathered during data collection, segmenting sentences (or paragraphs) […] into categories, and labelling those categories with a term".[134] Precisely the action of labelling is what permits the researcher to then build a thematic map in which the coded material is interpreted and placed under a specific theme. A process that overall appears to be applicable to a large variety of data. However, after an initial reading of the primary sources, the author has concluded that the process of coding might not be suitable to them. Indeed, within the strategies, specific passages and words linked to the field of cybersecurity connote some rather straightforward concepts or behaviours, leaving little room for an action of labelling or tagging, since specific words found within the documents act as labels themselves. Further, the author has come to the conclusion that many of the practices and actions presented in the primary sources overlap, something that would then produce codes without explicit boundaries, but rather redundant and interchangeable,

[133] Nowell, et al. "Thematic Analysis", 4.
[134] John W. Creswell, *Research design: Qualitative, quantitative, and mixed methods approaches* (SAGE Publications, Inc, 3rd edition, July 15, 2008), 186.

characteristics that should be avoided when producing codes.[135] Overall, rather than coding the data the author has surveyed it looking for specific discursive categories, passages and words that, as mentioned, carry a specific connotation derived from the cybersecurity field, which reoccur throughout the entire set of gathered data. Once gathered, the author has proceeded in clustering them under some specific sub-themes. Whether key words, expressions, and passages in the texts have been deemed rather straightforward in meaning, others have been set aside within an "in need of further interpretation" box, better evaluated vis-à-vis the gathered and utilised "technical" literature in cybersecurity and highlighted historical context. Given the nature of the practices and measures examined, the boundaries among some sub-themes are indeed blurred, a limitation that however is overcome by simplifying things, as explained in more details in the next chapter.

One final note regarding the sub-themes: drawing from qualitative content analysis, the number of times such discursive categories are repeated throughout the gathered data has been counted.[136]

Qualitative content analysis presupposes that specific terms maintain their meaning over time; the author believes that such an approach is able to provide further methodological rigour to the present dissertation methodology since within the cybersecurity field some words and expressions, as found within the primary sources, are commonly linked to

[135] Jennifer Attride-Stirling, "Thematic networks: an analytic tool for qualitative research", *Qualitative Research*, Vol. 1, No, 3 (2001), 385 - 405, 391.
[136] Klohs and Niemann, "Comparing the US National Security Strategy and the European Security Strategy in the first decade of the 21st century", 7.

specific actions, and understanding, that have not really changed over time. Adopting such method of enquiry grants the possibility to better assess whether specific terms and passages repeat themselves across the strategies. Such counting gives an initial glimpse into the degree of "intertextuality" of the selected data, helping visualising US cyber strategic thinking across time.

Once the sub-themes have been refined, the author has proceeded in sorting them under two opposite "normative thematic categories".

Such two thematic categories have been built following both an a-priori and inductive approach. When engaging the primary sources, the author already started with some initial knowledge on the field of cybersecurity and strategic thinking; something that produced some initial beliefs and ideas on what to look for within the documents. Precisely these initial ideas and beliefs have brought the author to conceiving the two "thematic normative categories". A-priori themes, as pointed out by some within the literature, tend to come from the characteristics of the topic being studied and analysed, as well as from professional definitions present within the literature, among others.[137] Further, it has been said that researchers can indeed argument their choices of a theme by referring to the literature.[138]

---

[137] Martin Bulmer, "Concepts in the analysis of qualitative data", *Sociological Review*, Vol. 27, No. 4 (1979), 651 - 677; Anselm L. Strauss, *Qualitative analysis for social scientists* (Cambridge University Press, 1987); Ryan and Bernard, "Techniques to Identify Themes", 88.

[138] Jodi Aronson, "A Pragmatic View of Thematic Analysis", *The Qualitative Report*, Vol. 2, No. 1 (1995), 1- 3.

Moreover, through the analysis of the content of the primary sources, the "story" of the "thematic normative categories" have been refined and further better explained.

The thesis follows the tradition that sees themes as "abstract entit[ies] that brin[g] meaning and identity to a recurrent experience and its variant manifestations".[139] Or put in a simpler way, as patterns of meaning that are able to capture something important to the overall research end goals,[140] also linking substantial portions of the data together.[141]

The two "thematic normative categories" have been named "defensiveness" and "offensiveness", as better explained in the upcoming chapter. The process of naming themes is a rather key one within thematic analysis, something that, as previously showed, is found almost at the end of the entire process. Nonetheless, given that in the present dissertation an a-priori approach was used, the author already had these names (thus themes) in mind when approaching the data. During the course of the research and writing process, for each of them the "story" they tell has been written, in order to further provide clarity to the reader and to the overall research process. The author also believes that approaching the data also

---

[139] Lydia DeSantis and Doris Noel Ugarriza, "The Concept of Theme as Used in Qualitative Nursing Research", *Western Journal of Nursing Research*, Vol. 22, No. 2 (2000), 351 - 372, 362.
[140] Braun and Clarke, "Using thematic analysis in psychology".
[141] DeSantis and Ugarriza, "The Concept of Theme as Used in Qualitative Nursing Research"; Nowell, et al. "Thematic Analysis", 8.

through such a deductive approach helps achieving themes that are internally coherent and do not overlap.[142]

Sorting the sub-themes under the two "thematic normative categories" by following also the chronological order of publication of the various primary sources helps understanding the overall evolution of US cyber strategic thinking, therefore when one specific norm seems to be informing the "cyber strategic culture".

Within the paper, the expression "normative thematic category/ies" and term "theme(s)" are used interchangeably.

4.6. A clarification on ACD and limitations of data and dissertation

Regarding the primary sources, it has been pointed out that despite what written in national strategies and official documents, states are still free to act differently, given that there might be differences between what an international actor signals and what it actually does. Nonetheless, they do provide valuable knowledge on how a state and some specific organisations within it strategically think regarding a specific domain and issue; hence on what kind of norms inform them. Further linked to such sources, unfortunately at this moment in history for cybersecurity and cyber warfare related matters, access to memoirs and decision-making processes is really difficult to achieve, not only due to the novelty of the domain and

[142] Braun and Clarke, "Using thematic analysis in psychology", 94 - 95.

strategic thinking about it, but also due to the still large veil of secrecy surrounding such processes at the national level. Precisely such a lack of more "intimate" data must be understood as a limitation to the analysis. To partially overcome such issue, elite interviews could have been set up and carried out, however some constraints prevented such a methodological technique to be adopted.

Regarding the methodology above-mentioned and the focus posed to so-called "active cyber defence" (ACD) measures, some more clarification is needed. In analysing their nature, the explained methodology has been fully applied, with the official discourse being analysed and the concept being processed through the two highlighted "thematic normative categories". To further push the analysis on ACD, thoroughly grasping all their facets, secondary sources have provided some more technical details and shared opinions on it; information that helped the author better understand such defensive paradigm's nature, thus allowing for a better interpretation and overall thematic analysis. Indeed, despite the discourse, as found in official strategies, only makes part of half the analysis on ACD, this latter still has been scrutinised though the two crafted themes. Moreover, whether grasping ACD's nature from opinions found within the literature might predispose the author towards certain biases, to further achieve objectivity some official US documents more or less linked to such concept have been taken into account.

Overall, the data gathered dates back to 2003, the moment when the White House published the very first cybersecurity strategy. Of course, the

discourse regarding cyberspace, cybersecurity, and cyber warfare is much more older, dating back to the 1980s, and especially 1990s (despite at that time other expressions and words were utilised to refer to such domain and possible military applications within it), as briefly mentioned in the literature review. Despite such temporal window taken into account being potentially perceived as a limit of the present dissertation, such a choice has been made due to time and word count constraints. Such a limit opens up more room for research, for instance a possible expansion of the work carried out here, comparing its results with those reached when taking into account also the two mentioned historical timeframes that came before the "militarization" one.

Regarding more technical aspects covered in the present thesis, the author being a scholar of IR and security studies does not have the competencies to fully explain more technical aspects of cybersecurity and defence. Accordingly, he understands that they might have been covered and explained in rather simple terms. Nevertheless, despite that potentially being perceived as a limit, in the opinion of the author the details given suffice in providing clarity for the sake of the argument and analysis presented in the dissertation.

Finally, as seen within the literature, scholars have pointed out the fact that the US still lacks a comprehensive cyber strategy. Such a "lack" must not be interpreted as a potential limit capable of invalidating the research agenda followed in the present paper. Having one holistic and comprehensive official document would have simplified the research process, providing

more empirical material to work with; however, the primary sources utilised do provide the data onto which apply the chosen methodology and theoretical axioms, tracing the norms that inform/mirror the US "cyber strategic culture".

5. Defining the analytical framework - the two "thematic normative categories"

As briefly introduced in the chapter on the methodology, two key major "thematic normative categories" form the methodological lenses through which the data corpus has been analysed. The present chapter aims at better explaining the "story" of such themes, presenting their related sub-themes, explaining also some technical and strategic aspects of those techniques and measures falling within them.

5.1. "Defensiveness"

The "story" of this theme is one of non-aggressiveness. A discourse characterised by measures and practices that neither directly nor overtly signal the willingness to harm other actors or their networks, systems, and infrastructure. Overall, the literature on cybersecurity offers some initial insights into the various measures actors can take to increase the defences and security of their networks and systems without directly decreasing that of adversaries. Accordingly, a set of a-priori sub-themes has been delineated, namely: network security/defence, cyber-resilience, and cooperation.

Before proceeding, it is mandatory to point out that the boundaries between such sub-themes are not definable with maximum certainty, since some of the practices contained in each of them might overlap, or at least

possibly fall in more than one of them. Nonetheless, for the sake of clarity a rather clear-cut division is here presented.

5.1.1. Network security/defence

To avoid malicious actors entering networks, thus data present on them as well as systems connected to them, experts speak of strengthening and fortifying networks,[143] two verbs also present in the assessed primary data.
The first sub-theme, which has been called network security/defence, is linked with tools and software, both reactive and proactive in nature,[144] that are implemented precisely to defend networks as well as data, devices, and systems present and connected to them, from malicious intrusions.
Central to this sub-theme is the capacity for a network and system to defend its perimeter, keeping threats outside of it, as well as that of preventing further spreading of malevolent software, which managed to breach through the initial defences.

The literature often points to the concept of "layered defence", a term that indicates the presence of a multitude of layers each implemented on top of

[143] Robert S. Dewar, "The Triptych of Cyber security: a classification for active cyber defence", in *2014 6th International Conference on Cyber Conflict: Proceeding*, edited by P. Brangetto, M. Maybaum, J. Stinissen (NATO CCD COE Publications, 2014), 7 - 22.
[144] The differentiation between reactive and proactive measures taken regarding cyber-related issues is a recurring one within the present thesis; for instance, such a differentiation is better taken under scrutiny in the chapter dedicated to "active cyber defence" measures.

the other to slow down attackers and malicious activities.[145] Accordingly, in simple terms it is possible to speak of perimeter and internal defences. Presenting an exhaustive list of all implementable measures and respective characteristics is well beyond the scope of the present chapter and not really useful to the overall bottom line of the thesis. Nonetheless, some general insights on some of the most common techniques are here presented, especially to better distinguish this first sub-theme from the next ones.

One of the first measures often underlined in the literature are so-called firewalls, the digital version of real-life barricades and barriers. Such tools are designed to prevent the protected computers from establishing potentially malevolent connections and from carrying out certain activities, thus acting as filters permitting only those actions deemed valid.[146] Such a measure is one of the simplest external defences that can be implemented. As pointed out by the literature, the practice of filtering, once thought impossible, is now widespread, adopted globally at various levels.[147]

Antivirus are another rather common measure in network security, often applied at multiple levels in a network. Such tools function by scanning all files present on a system, as well as the incoming traffic, looking for known

---

[145] Jerry Shenk, "Layered Security: Why It Works", *SANS Institute* (2013), 5. Available at: https://www.sans.org/reading-room/whitepapers/analyst/layered-security-works-34805.

[146] Singer and Friedman, *Cybersecurity and Cyberwar*, 62.

[147] Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security", *International Political Sociology*, Vol. 4, No. 1 (March, 2010), 15 - 32, 24.

"signatures", bits of code that are known for being associated with a specific malicious software ("malware").[148] Once detected such malicious software can be quarantined and deleted before wreaking damage.

Similarly, so-called "intrusion detection systems" (IDPs) also are tools, or better, sensors that monitor network traffic for malicious activity.[149] Further, their direct successors, called "intrusion prevention systems" (IPSs), not only monitor but can also directly and in an automated fashion block suspicious network traffic. These latter implement more detection methods than antivirus, being able to protect against still unknown threats. Indeed, IPSs can detect malicious activity before antivirus signatures are created and implemented for them.[150]

Given that cyber threats update continuously, defenders need to always keep pace. For this reason, important measures falling under the umbrella of network security/defence involve patch management and antivirus updates.[151] These consist of updating the list of known malicious software and threats, and applying upgrades to the owned systems and networks to increase their robustness and fix known weaknesses and potential points of entrance for malicious actors. Such two measures are linked to the human layer, therefore to the level of awareness and preparation of a workforce;

---

[148] Singer and Friedman, *Cybersecurity and Cyberwar*, 60 - 61.
[149] James Graham, Richard Howard, and Ryan Olson, *Cyber Security Essentials* (Auerbach Publications, 2011), 295.
[150] Mikko Särelä et al., "Evaluating intrusion prevention systems with evasions", *International Journal of Communication Systems*, Vol. 30, No. 6 (November, 2017).
[151] Singer and Friedman, *Cybersecurity and Cyberwar*, 62 - 63.

something that is achieved through sound training. As later shown, the human layer is also important within the next sub-theme.

Overall, even if the measures described are implemented, experts agree that malicious actors still manage to bypass cyber fortifications. Precisely for this reason defenders need to be ready to act even when under attack, coping with the consequences.

5.1.2. Cyber-resilience

Resilience is the second sub-theme making up the "story" of the "defensiveness" normative thematic category. Such a term has become central in many security fields, utilised widely in different contexts and vis-à-vis various threats. With the advent of the World Wide Web and the increasing reliance of societies and firms to the Internet and cyber medium, resilience also has started to become a rather central topic in the cybersecurity discourse.

Within the cybersecurity field, the literature confirms that such a term lacks a universally accepted definition,[152] with various authors taking into

[152] Myriam Cavelty Dunn, Mareile Kaufmann, and Kristian Søby Kristensen, "Resilience and (in)security: Practices, subjects, temporalities", *Security Dialogue*, Vol. 46, No. 1 (2015), 3 - 14.

account different dimensions, characteristics, and practices when conceptualising it.[153]

Nonetheless, a general common understanding defines such a concept as the capacity to handle threats when these materialise and regain either the initial or a new normal functioning in the least time possible.[154] Similarly, the 2010 US National Security Strategy defines it as "the ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption".[155]

By applying such conceptualisations to the cyber domain a simple definition of cyber-resilience is reached, namely the ability of systems, networks, and related infrastructures to sustain a cyberattack, maintain their functioning even when under attack, withstand it, and quickly recover from it.[156]

---

[153] Leire Labaka, Josune Hernantes, and Jose M. Sarriegi, "A holistic framework for building critical infrastructure resilience", *Technological Forecasting & Social Change*, Vol. 103 (2016), 21 - 33, 22.
[154] Eviatar Matania, Lior Yoffe, and Michael Mashkautsan, "A Three-Layer Framework for a Comprehensive National Cyber-security Strategy", *Georgetown Journal of International Affairs*, Vol. 17, No. 3 (Fall/Winter 2016), 77 - 84, 80.
[155] White House, *National Security Strategy 2010* (Washington DC, White House, May 2010), 18.
[156] Daniel Dobrygowski, "Cyber resilience: everything you (really) need to know", *World Economic Forum*, July 8, 2016 (accessed June 2018), https://www.weforum.org/agenda/2016/07/cyber-resilience-what-to-know/.

It goes without saying then that resilience in cyberspace is something different from strict cybersecurity,[157] a word that better fits the previously mentioned measures,[158] since it involves more than software and hardware. Resilience indeed is a matter or people and processes, rather than just one of architecture and organisation.[159] Indeed, for it to be truly reached, there needs to be an intentional capacity to work even when conditions are not optimal or degraded, coupled with both a technical and behavioural predisposition to recover as soon as possible, learning lessons to better face future similar events.[160] Overall, experts underline some specific steps organisations can take to bolster their cyber-resilience preparedness, which involve good policymaking and management, behavioural and cultural aspects, as well as more technical ones.[161]

One initial step involves the awareness regarding the kind of information, systems, and infrastructures that need to be protected, from the most to the least important. Having a clear picture of the assets that need to be guarded and defended, with priorities clearly given, opens the door to better

---

[157] Jake Olcott, "Cybersecurity Vs. Cyber Resilience", *Bit Sight*, December 7, 2017 (accessed June 2018), https://www.bitsighttech.com/blog/cyber-resilience.

[158] Darko Galinec, Darko Možnik, and Boris Guberina, "Cybersecurity and cyber defence: national level strategic approach", *Automatika*, Vol. 58, No. 3 (2017), 273 - 286.

[159] Singer and Friedman, *Cybersecurity and Cyberwar*, 173.

[160] Ibid., 171.

[161] Cisco, *Cyber Resilience: Safeguarding the Digital Organization* (2016), available at: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cyber-resilience-safeguarding-digital-org-wp.pdf; World Economic Forum, *Advancing Cyber Resilience Principles and Tools for Boards* (January 2017). Available at: http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf.

decision-making. Secondly, clear policy guidelines need to be implemented, with roles and responsibilities clearly defined, giving equal importance to people, processes, and technology. Both these two initial steps help speeding up the entire response process. Thirdly, given that most experts still consider the human factor the "soft underbelly" of cybersecurity, sound training and awareness raising programs are fundamental measures to be implemented to enhance cyber-resilience,[162] since they not only raise awareness on the overall network infrastructure present within an organisation, but also teach the workforce best cyber hygiene practices, such as to regularly back up their files.[163]

Finally, from a more technical point of view, one simple step to enhance cyber-resilience is to make networks redundant, duplicating their components to increase reliability.[164] Further, organisations can implement new and more resilient systems, which are characterised by faster and simpler recovery procedures to a previous or new state of integrity.[165] Finally, running red-team exercises, penetration tests to discover potential vulnerabilities, also enhances cyber-resilience.[166]

---

[162] Nick Wilding, "Cyber resilience: How important is your reputation? How effective are your people?", *Business Information Review*, Vol. 33, No. 2 (2016), 94 - 99.
[163] Olcott, "Cybersecurity Vs. Cyber Resilience".
[164] Singer and Friedman, *Cybersecurity and Cyberwar*, 171.
[165] Igor Linkov et al., "Resilience metrics for cyber systems", *Environ Syst Decis,* Vol. 33 (2013), 471 - 476, 473.
[166] Warwick Ashford, "UK leading in using red team cyber security testing", *Computer Weekly*, March 31, 2017 (accessed June 2018), https://www.computerweekly.com/news/450416013/UK-leading-in-using-red-team-cyber-security-testing.

5.1.3. Cooperation

The third and final sub-theme of the "defensiveness" "thematic normative category" is centred around cooperation practices. These can happen both at the national and international level, with the primary aim of bolstering overall awareness and knowledge of cyber threats and risks, thus preparedness and capabilities to repeal, manage, and recover from attacks and malicious intrusions. Indeed, such sub-theme, as already hinted, finds a close linkage with the two already explained sub-themes, cyber security/defence and cyber-resilience.

At the domestic level, cooperation takes place (and is needed further) between private firms, government, federal departments, and agencies. However, much more emphasis is posed on cooperative efforts between the public and private sector. The so-called concept of Private-Public Partnerships (PPPs) has been around since the second half of the 20th century, being presented as a silver bullet to various problems in many fields, but also receiving some criticism across time.[167] Explaining the "lights and shadows" of PPPs is beyond the scope of the present dissertation, nonetheless important is that in recent years such a concept conquered a central position within the cybersecurity discourse, with many official national strategies underlying the importance of achieving sound

[167] Myriam Cavelty Dunn and Manuel Suter, "Public-Private Partnerships are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection", *International Journal of Critical Infrastructure Protection*, Vol. 4, No. 2 (2009), 179 - 187, 180.

cooperation, especially in regards to critical infrastructures protection (CIP).[168]

At the international level, cooperation in the field of cybersecurity and cyber defence has become a major topic of discussion as well, especially between countries pertaining to an international organisation or alliance. For instance, the importance of achieving sound cooperation between states has been discussed and pushed forward both at the European Union and NATO level.[169]

In simple terms, the main point of cooperating and creating partnerships is primarily that of sharing actionable knowledge and awareness, such as information collected from suffered cyber attacks; or in jargon "threat intelligence". Such information is the "good" that experts point out needs to be shared in order to enhance overall cybersecurity.[170] Moreover, also

---

[168] Madeline Carr, "Public–private partnerships in national cyber-security strategies", *International Affairs*, Vol. 92, No. 1 (2016), 43 - 62.

[169] ENISA, *Cybersecurity cooperation: Defending the digital frontline* (October 2013), available at: https://www.google.cz/search?q=cooperation+is+key+cybersecurity&oq=cooperation+is+key+cybersecurity&aqs=chrome..69i57.4646j1j7&sourceid=chrome&ie=UTF-8#; Warwick Ashford, "Cooperation and exercises key to cyber defence, says Nato centre", *Computer Weekly*, March 9, 2018 (accessed June 2018), https://www.computerweekly.com/news/252436575/Cooperation-and-exercises-key-to-cyber-defence-says-Nato-centre. Here, a key topic is that of norm promotion and norm emergence, something not directly taken into account in the present dissertation, as already pointed out.

[170] Itzik Kotler, "The Key To Cybersecurity: Shared Intelligence And Industry Cooperation", *Forbes*, February 11, 2017 (accessed June 2018), https://www.forbes.com/sites/forbestechcouncil/2017/02/15/the-key-to-cybersecurity-shared-intelligence-and-industry-cooperation/#3ecb5e2c7eb8.

experience and best practices on how to defend and recover from an attack are key "goods" that need to be shared.

Finally, cooperation has been utilised as diplomatic tool to increase bilateral and multilateral relationships among countries that might see each other as adversaries under certain lenses. In other words, sharing information can be utilised as a confidence building mechanism, a vehicle through which signal good intensions and enhance mutual relationships.

5.2. "Offensiveness"

If the "defensiveness" thematic normative category connotes a "story" of measures taken to bolster one cybersecurity without necessarily harming an adversary, the second thematic normative category crafted in the present dissertation, "offensiveness", narrates precisely the opposite.

On a general level, the term "offence" connotes an image of an action undertaken to hurt something or someone else. Indeed, such term's etymology comes from the Latin word "offendere", which can be translated with the expression/verb "to strike against".[171]
The meaning of such a term is in reality broader than what mentioned, encompassing also actions that might not be violent per-se.[172] Despite that, in the present dissertation of interest is the highlighted meaning and

[171] Merriam-Webster, "Offense", *Merriam-Webster,* (accessed June 2018), https://www.merriam-webster.com/dictionary/offense.
[172] For instance, prosecuting acts from a strictly legal point of view, both at the domestic and international level.

etymology, which serves as a guiding framework for the creation of this "offensiveness" "story".

One that shares a bridge with the logic of zero-sum, since it is explained by the threat or use of force, and practices that by increasing the security of one actor decrease that of others, creating the so-called "(cyber) security dilemma". Overall, the "story" of this second thematic normative category encompasses a discourse and strategic thinking that favour offensive cyber capabilities over defensive ones, thus an offensive use of the medium itself, as well as that signal a willingness to go aggressive towards adversaries on a broader and general level. Arguably, the "story" of "offensiveness" appears also closely tied to the notion of "cyber war".[173]

Whether for "defensiveness" three key sub-themes have been highlighted, all linked to both technical and non-technical cybersecurity measures and practices, for the one presented in the following paragraphs such a clear distinction between measures and practices might not be possible to be drawn. Indeed, despite some sub-themes being presented, the ways to achieve their intended results all adopt more or less the exact same tools, namely weapons that are designed to be exploited aggressively against menaces/threats and adversaries, which can either be kinetic or cyber in nature. For the sake of clarity, "cyber weapons" needs to be defined. As pointed out by Stevens, a universally accepted definition of such kind of

---

[173] The notion of "cyber war" is a rather debated one. Within the present dissertation the one offered by Clarke and Knake is deemed sufficient: "actions by nation-states to penetrate another nation's computers or networks for the purposes of causing damage or disruption". Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (Ecco; Reprint edition, August 5, 2011), 6.

weapons still is lacking, with the term having been utilised as a catch-all phrase indicating a rather large set of malware said to be capable of various effects.[174] In the present dissertation cyber weapons are conceptualised as "tool[s] (computer code) that [are] used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings". [175] Also, especially to better understand the analysis of "active cyber defence" measures, it must be pointed out that in cyberspace the concept of border/boundary is not as straightforward definable as it is for more traditional domains, being debated and subject to dispute. Nonetheless, for the sake of clarity, the present dissertation overlooks such issue concentrating rather on the already defined definitional distinction between techniques that relate to an actor's own systems and those that do not.[176]

5.2.1. Preemption/Prevention

The notions of preemption and prevention form the first sub-theme forming the "story" of "offensiveness", two terms often grouped under the umbrella of "anticipatory action/attack".[177] Despite being linguistically very close one to the other, such two terms have rather different connotations,

---

[174] Tim Stevens, "Cyberweapons: An Emerging Global Governance Architecture", *Palgrave Communications*, Vol. 3 (January 2017).
[175] Thomas Rid & Peter McBurney, "Cyber-Weapons", *The RUSI Journal*, Vol. 157, No. 1 (2012), 6 - 13, 7.
[176] Paul Rosenzweig, "International Law and Private Actor Active Cyber Defensive Measures", *Stanford Journal of International Law*, Vol. 50, No. 1 (Winter, 2014), 103 - 118, 106.
[177] Karl P. Mueller et al., *Striking First: Preemptive and Preventive Attack in U.S. National Security Policy* (RAND, 2006), xii.

depicting two distinct strategic behaviours. Indeed, from a strategic thinking point of view, if on one hand to preempt means using military force firstly "when an enemy attack already is underway or, at the least, is very credibly imminent";[178] on the other, as Brodie puts it, prevention entails "a premeditated attack by one country against another, which is unprovoked in the sense that it does not wait upon a specific aggression or other overt action by the target state".[179] In other words, to prevent entails attacking first not due to an imminent attack, but to avoid a possible future re-balancing of the status quo, which might puts an adversary in a more favourable position.[180] Regarding the US, the discourse on such two terms, hence strategic thinking, can be traced back to the initial stages of the Cold War. Whether a differentiation between the two of them existed during the 20th century, with the turn of the millennium, the 9/11 attacks, and the Bush Presidency, the boundaries between the two terms became blurred, with the term preemption being utilised to connote also its counterpart. [181] Indeed, the 2002 National Security Strategy defines preemption in rather broad and general terms as "striking first against perceived security threats under a variety of circumstances".[182]

---

[178] Colin S. Gray, *The Implication of Preemptive and Preventive War Doctrines: A Reconsideration* (Strategic Studies Institute, US Army War College, July, 2007), 8.
[179] Bernard Brodie quoted in Harry S. Laver, "Preemption and the Evolution of America's Strategic Defense", *Parameters*, Vol. 35, No. 2 (Summer, 2005), 107 - 120, 112.
[180] Jack S. Levy, "Preventive War and Democratic Politics", *International Studies Quarterly*, Vol. 52, No. 1 (March, 2008), 1 - 24, 1.
[181] Michael E. O'Hanlon et al., "The New National Security Strategy and Preemption", *The Brookings Institution - Policy Brief*, No. 113 (December, 2002). Available at: https://www.brookings.edu/wp-content/uploads/2016/06/pb113.pdf.
[182] Mueller et al., *Striking First*, xi.

5.2.2. Retaliation

The second sub-theme is that of retaliation. From a strategic point of view such a term means acting after having suffered an initial attack, launching a counter-attack. Within the US, such a term has been mostly linked to the logic of deterrence, being a key tile within the logic of "mutual assured destruction" (MAD). Such a possible strategic behaviour has been also transposed to the cyber medium, precisely to the concept of cyber-deterrence, a rather debated one, which sees experts and academics split in two.[183] Despite some scepticism being raised in regards of the feasibility of sound retaliation in cyberspace due to malicious actors' possibility to hide their identity,[184] such a practice is at the centre of a rather topical debate.

5.2.3. Domination

The third and last sub-theme is that of domination, which from a strategic point of view entails a willingness to dominate a specific domain of warfare, maintaining the upper hand and denying it to perceived

[183] On the possibility to achieve deterrence in cyberspace much has been written. One of the most important piece of writing on the topic, which the author recommends, is the following: Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, RAND, 2009).

[184] Such a debate is far from reaching an end. On one side there are those who argue that the technical characteristics of the cyber medium does not permit to pinpoint the perpetrator with 100% certainty, while on the other there are those who argue that thanks to an analysis of the geopolitical scenario, self-interests, past behaviour etc., pointing the finger is a rather straightforward political act, which can still be achieved also for cyber operations.

adversaries; precisely something that entails a disparity in capabilities, thus in security as well. Of course to dominate also means being able to resist an attack, however much more emphasis is given to the development of aggressive means capable to give one actor an advantage over another. This sub-theme shares some similarities/overlaps with that of preemption/prevention, since to some extent it also entails the possibility to carry out some operations first, nonetheless it is explained as something different. Further, it also finds a link with the notion of cyber-power, since this latter is here understood as "the ability to control and apply typical forms of control and domination of cyberspace".[185]

Easier said than done, cyberspace is a much more complex domain than the most common ones, land, air, and maritime. Being entirely man made it presents some characteristics and peculiarities,[186] which undermine the possibility to achieve a high degree of persistent domination. Libicki divides the medium into three specific layers: 1) a physical one, entailing hardware that participate in making cyberspace exist; 2) a syntactic one, which consists in all those software-operational instructions and rules that are provided to the physical layer; and finally, 3) a semantic one, grouping the vast amounts of data and information that flow across the ether of cyberspace, hence through its physical nodes.[187] Each of these layers is

[185] Valeriano and Maness, *Cyber War versus Cyber Realities*, 28.
[186] John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War", *Strategic Studies Quarterly*, Vol. 5, No. 2 (Summer, 2011), 95 - 112, 96 - 100.
[187] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge University Press, 2007), 8 - 9.

dominated by exploiting different aggressive measures. Further, one needs to act on all of them, since "conquering" one does not necessarily mean dominating the others.[188]

Leaving such vast debate aside, in following Sun Tzu's thought, many scholars point out that in cyberspace to truly achieve the upper hand and dominate it is mandatory to have a complete knowledge of the adversary's offensive and defensive capabilities. Achieving so requires the gathering of intelligence, which within the cyber medium is done through so-called Computer Network Exploitation (CNE) operations. Since according to the literature the practice of intelligence gathering is the norm in interstate relationships,[189] with the cyber medium only having opened the door to a larger amount of information to be potentially gathered, and the US having a long lasting legacy and interest in such a practice,[190] domination from that point of view is not taken into account. Rather, what is understood as the sub-theme of domination is a form of "operational preparation of the cyber battlefield" (OPB). A practice that entails an aggressive breaching of adversaries' networks and systems and the placement of so-called logic

---

[188] Ibid.

[189] Martin C. Libicki, "Sub Rosa Cyber War", in *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by C. Czosseck and K. Geers (IOS Press, 2009), 53 - 87.

[190] Shannon Tiezzi, "The US and China's Common Interest: Cyber Spying", *The Diplomat*, December 11, 2013 (accessed June 2018), https://thediplomat.com/2013/12/the-u-s-and-chinas-common-interest-cyber-spying/; Lothar Determann and Karl-Theodor zu Guttenberg, "Spies Will Be Spies in War, Peace and Cyberspace", *Huffington Post*, September 13, 2014 (accessed June 2018), https://www.huffingtonpost.com/lothar-determann/cyberspace-spies_b_5583006.html?guccounter=1.

bombs and trapdoors,[191] which give a rather high degree of strategic advantage, hence domination. Indeed, whether trapdoors can be understood as secret openings left behind by attackers in adversaries' networks to be later exploited to quickly regain access to them;[192] logic bombs are "piece[s] of code inserted into a software system that can lie dormant and undetected for extended periods of time […] activated to perform some malicious function [at a later moment]".[193]

Domination in cyberspace is often understood as the possibility to conduct operations in a safe way, "without prohibited interference by an adversary",[194] or more precisely as the "degree of dominance one force holds over an adversary that permits freedom of action in cyberspace at a given time and place while denying the same to that adversary".[195] Something that according to the view adopted in the present dissertation can indeed be achieved through the aggressive measures mentioned, since they provide a strategic head start, hence diminishing the possibility to be interfered when carrying out cyber operations. In fact, some experts draw a parallel between air and cyber superiority. In this latter, commanders

---

[191] Clarke and Knake, *Cyber War*, 31.
[192] Stephen Northcutt, "Security Laboratory: Methods of Attack Series", *SANS*, May 2, 2007 (accessed June 2018), https://www.sans.edu/cyber-research/security-laboratory/article/log-bmb-trp-door.
[193] Christopher J. Eberle, "Just War and Cyberwar, *Journal of Military Ethics*, Vol. 12, No. 1 (2013), 54 - 67, 62.
[194] Lt Col William D. Bryant (USAF), "Cyberspace Superiority: A Conceptual Model", *Air & Space Power Journal*, Vol. 6, No. 6 (November–December, 2013), 25 - 44, 39.
[195] Han Bouwmeester, Hans Folmer & Paul Ducheine, "Cyber Security and Policy Responses", in *Cyber Warfare: Critical Perspectives*, edited by Paul Ducheine, Frans Osinga, and Joseph Soeters (t.m.c. Asser press, 2012), 19 - 48, 28.

before green lighting a strike needs to be sure that the defensive systems deployed by the enemy have been suppressed, in order to lower the possible resistance to the raid by the enemy. In a similar fashion, when a cyber operation is planned against an adversary's system or network, commanders may want to firstly "attack the enemy's computer systems to [nullify its] ability to penetrate and disrupt [the] information and communication networks [utilised in conducting the attack]".[196] Precisely for this reason, according to DOD's Joint Concept on Cyberspace (JCC), domination in cyberspace can be achieved also through Offensive Cyber Operations (OCOs).[197]

[196] Tom Gjelten, "First Strike: US Cyber Warriors Seize the Offensive", *World Affairs*, January/February 2013 (accessed June 2018), http://www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive.

[197] Bouwmeester, Folmer & Ducheine, "Cyber Security and Policy Responses", 28.

6. A "cyber strategic culture" dominated by "defensiveness"

The present chapter seeks to demonstrate that across the analysed data corpus the three-sub themes that participate in creating the "story" of the "defensiveness" "thematic normative category" constantly appear, occupying a rather central spot within the general cyber-related narrative. Precisely their consistency across time is understood as a proof that the US cyber strategic culture is predominately and continuously informed by a norm of "defensiveness". A result rather in line with what already stated by some scholars within the literature.[198] The analysis of the discourse of the data corpus points out that all three "defensiveness" sub-themes are present

[198] Dunn Cavelty, "Breaking the Cyber-Security Dilemma", 702. The author would like to remind that this result, despite making half of the analysis of the present dissertation is not the key one, which is rather the one centred around the discursive demonstration of the norm of "offensiveness" informing the US "cyber strategic culture".

in nearly all official documents. Indeed, there is consistency between the documents published by the White House and military as well.

6.1. White House

One of the richest documents in terms of information and discursive evidence is the 2003 National Strategy to Secure Cyberspace. Among the various measures to implement, focus is especially given to the creation of a "multi-layered defence" and resilient networks. Several references are furthermore made to patch management, vulnerabilities reduction, damage and recovery times minimisation, and deployment of systems less vulnerable;[199] all of which can be interpreted precisely as falling within the first two sub-themes of "defensiveness". Furthermore, the 2003 official document also highlights the need to share information both at an interagency level, with the private sector, and internationally with allies.[200]

The second most important document published by the White House regarding cybersecurity is the 2011 International Strategy for Cyberspace. The discourse found in it also puts the accent on the need to strengthening network defences and the capability to withstand and recover from cyber attacks, isolate and mitigate disruption, and share information and early warning capabilities. Therefore presenting all three "defensiveness" sub-

[199] White House, *The National Strategy to Secure Cyberspace* (Washington, DC, February, 2003), 14, 29 - 35, 43 - 48.
[200] Ibid., 24 - 25, 48, 50 - 52.

themes. Such document states the following: "[t]he United States will continue to strengthen our network defenses and our ability to withstand and recover from disruptions and other attacks. For those more sophisticated attacks that do create damage, we will act on well-developed response plans to isolate and mitigate disruption to our machines, limiting effects on our networks, and potential cascade effects beyond them".[201]

The various points highlighted in 2003 and 2011 can be found in various National Security Strategies (NSS) as well.[202] For example, the 2010 NSS, despite remaining rather vague, highlights the importance to achieve resilient networks, design (and implement) more secure technology, defend networks from intrusion and disruption, as well as build and sponsor awareness, and especially domestic and international cooperation.[203] The NSS published in 2015, focusing much on critical infrastructure protection, adopts the verb "fortifying" also within the context of cybersecurity; a term connected to network security/defence, stating that the US is "fortifying [its] critical infrastructure against all hazards, especially cyber espionage and attack".[204] In addition, such official documents also shares an overall discourse linked to resilience and cooperation as well, stating that actions are being undertaken by "working with the private sector, civil society, and

---

[201] White House, *International Strategy for Operating in Cyberspace. Prosperity, Security, and Openness in a Networked World* (Washington, DC, May, 2011), 12 - 13.

[202] There is one exception here, namely the 2006 NSS. Such a document was not taken into account since it lacks a cybersecurity discourse. Indeed, the word "cyber" only appears once.

[203] White House, *National Security Strategy 2010*, 18, 27 - 28, 50.

[204] White House, *National Security Strategy 2015* (Washington, DC, February, 2015), 3.

other stakeholders to strengthen the security and resilience of U.S. critical infrastructure".[205]

In the latest 2017 NSS, again several sentences and words utilised point to resilience, network security/defence, and cooperation.[206] Resilience truly stands out for importance, indeed on a more general level an entire sub-section is dedicated to it, with the document stating that building a culture of resiliency across multiple US systems, from economic to political ones, is a "key goal".[207] Such an importance is then mirrored also regarding cyberspace, with resilience being stressed within the context of government, private networks, and national critical infrastructures. For instance, the 2017 NSS states the willingness to achieve "uninterrupted and secure communications and services under all conditions".[208] Interestingly, the 2017 NSS clearly underlines the importance of prioritising the infrastructures, systems, and data to be secured, which, as explained in the previous chapter, is a key step to increase the overall degree of resilience. In the official document words: "[t]o improve the security and resiliency of our critical infrastructure, we will assess risk across six key areas […]. We will assess where cyberattacks could have catastrophic or cascading consequences and prioritise our protective efforts, capabilities, and defenses accordingly".[209] Furthermore, the 2017 NSS underlines the need for a new forward-looking ethic to secure and enhance resiliency of the country's

[205] Ibid., 9, 12.
[206] White House, *National Security Strategy 2017* (Washington, DC, December, 2017), 13, 48.
[207] Ibid., 7.
[208] Ibid., 13.
[209] Ibid.

critical infrastructures, namely the fact that such a condition needs to be implemented right from the start, rather than simply added afterwards since malicious actors can exploit such a temporary gap within the infrastructure.[210] Regarding network security/defence, the 2017 NSS clearly speaks of "layered defences", which must be deployed in order to avoid the spread of malicious activity, which "must be defeated within a network and not be passed on to its destination whenever possible".[211] Finally, regarding the third sub-theme, in line with the previous White House documents, also the latest NSS stresses the importance of cooperating, both domestically with the private sector and internationally with allies to bolster cybersecurity readiness and defences.[212]

6.2. Military

With the exception of the 2004 National Military Strategy (NMS), most documents published by the military display a discourse also filled by such a narrative, which persisted throughout time.

The originally secretive 2006 NMS for Cyberspace Operations clearly underlines the importance of achieving "redundancy, restorative capacities, consequence management",[213] a "layered defense-in-depth approach",[214]

[210] Ibid.
[211] Ibid.
[212] Ibid.
[213] Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations* (Washington, DC, December, 2006), 10.
[214] Ibid., 14.

"partnerships to increase resilience",[215] "sensors to detect malicious activity",[216] and "self-healing capabilities",[217] among others; all discursive references that do fall underneath the three sub-themes of "defensiveness", networks security/defence, resilience, and cooperation.

The 2011 DOD's Strategy for Operating in Cyberspace, also contains key passages that highlight a discourse centred mostly on "defensiveness". Initially such document explains that CYBERCOM has been established to answer specific DOD needs, such as building resiliency and smart partnerships.[218] In addition, the document speaks of the importance of cyber hygiene best practices, and the adoption of adaptive and dynamic network defences, as well as interagency and international collaboration.[219] For example, the strategy states a continuous usage of "advanced sensors to detect, discover, map, and mitigate malicious activity on DOD networks",[220] and that "[b]y sharing timely indicators about cyber events, threat signatures of malicious code, and information about emerging actors and threats, allies and international partners can increase collective cyber defense".[221] This document is truly important for the analysis conducted within the present dissertation, since it highlights how the DOD underwent a "shift" in its approach to cybersecurity, embodied in the adoption of "cyber active defence" (ACD) measures. In fact, as it is better

---

[215] Ibid., 16.
[216] Ibid., F - 1.
[217] Ibid., F - 2.
[218] Department of Defense, *The Department of Defense Strategy for Operating in Cyberspace* (Washington, DC, July, 2011), 5.
[219] Ibid., 6 - 10.
[220] Ibid., 7.
[221] Ibid.

shown in a following chapter, such a paradigm not only entails "defensiveness", but also entails some specific measures and tools, which do fall underneath the umbrella of "offensiveness". Given the complexity and centrality of ACD, the author decided not to split the discussion on it, presenting it within one unified chapter. Despite this latter being placed within the discussion of "offensiveness", here only a brief mention on the fact that ACD is a vehicle for "defensiveness" serves the purpose, with the actual analysis carried out in a dedicated sub-section of the next chapter.

The NMS of the same year also is full of discursive proofs of "defensiveness", making references to practices and measures falling within all three sub-themes of such first "normative thematic category", such as "multi-layered defense",[222] resiliency,[223] and cooperation.[224]

Whether the 2015 NMS only shares some mild references to the need to protect networks and infrastructures,[225] the 2015 DOD's Cyber Strategy more or less reprises what stated in 2011. There is a clear discourse centred around the sub-theme of network defence/security, with the strategy stressing that "DoD conducts network defense operations on an ongoing basis to securely operate the Department of Defense Information Network (D[O]DIN), [responding quickly when] indications of hostile activity within [DOD's] networks [are detected] [closing and mitigating]

---

[222] Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2011* (Washington, DC, February 8, 2011), 19.
[223] Ibid.
[224] Ibid., 9.
[225] Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2015* (Washington, DC, June, 2015), 7.

vulnerabilities and secur[ing] […] networks and systems".[226] The sub-theme of resilience is reprised and paralleled to the need of building redundant networks to achieve continuation of operation even when under attack or in degraded conditions.[227] Further, to increase readiness and discover vulnerabilities and weaknesses the practice of red-teaming is said to be conducted.[228] Finally, the sub-theme of cooperation is also present, with the official strategy pointing out the willingness of DOD to cooperate with allies from various regions of the world.[229]

In conclusion, as already mentioned, despite not fully reported here, there are other primary sources that highlight the preponderance of "defensiveness" sub-themes within US cyber strategy culture. For instance, more empirical discursive proofs of it can be gathered by assessing the following official documents: PPD - 21, Department of Homeland Security Quadrennial Reviews and Blueprint for a Secure Cyber Future, as well as President Barack Obama 2009 Cyberspace Policy Review. As already explained, such documents have been left out of the analysis because their implementation would not have dramatically altered the obtained results. Nonetheless, they have been mentioned in order to enhance the overall transparency of the thesis.

---

[226] Department of Defense, *The DOD Cyber Strategy* (April, 2015), 4.
[227] Ibid., 11.
[228] Ibid., 21 - 22.
[229] Ibid., 26 - 27.

7. "Offensiveness" - an increase of it within the US "cyber strategic culture"

In the timeframe under scrutiny in the present dissertation, key discursive passages found within the documents, coupled with the implementation of the already mentioned "active cyber defence" (ACD) measures, participate in showing how the US "cyber strategic culture" in recent years seems to be increasingly informed by "offensiveness". This chapter, which can be considered as the fulcrum of the present dissertation, seeks to highlight precisely that. Before proceeding onwards with the analyses of ACD, the 2015 DOD's Cyber Strategy, and the latest 2017 NSS, forming the real centre of the present thesis' argument, some other key documents that do display "offensiveness"-related sub-themes are briefly analysed.

7.1. "Offensiveness" before ACD, DOD's 2015 Cyber Strategy, and 2017 NSS

7.1.1. White House

Interestingly, before the 2017 NSS, only two other documents published by the White House do display some mild hints of aggressiveness.
For instance, the 2011 Strategy for Operating in Cyberspace underlines that "[w]*hen warranted,* the United States will respond to hostile acts in cyberspace as [it] would to any other threat to [the] country[, reserving] the right to use all necessary means – diplomatic, informational, military, and economic – as appropriate and consistent with applicable international

law, in order to defend [the] Nation, [its] allies, [its] partners, and [its] interests".[230] Further, the 2015 NSS points to the willingness of the US to "impose costs [vis-à-vis a cyber aggression] on cyber malicious actors".[231]

Such a discourse arguably highlights the presence of the sub-theme of retaliation. Using words such as "respond" and "impose costs" within the context of military power does connote the possibility to adopt force against a menace coming from cyberspace.[232] Such documents remain rather vague, with the discourse not really giving much more details on how such a response would play out. It is stated that the US will act in accordance with international law, indeed as pointed out by experts and scholars, political and military circles within the US do share the opinion that the rules governing armed conflict do find an application also in cyberspace. Going into details into such a topic is well beyond the scope of the present dissertation, nonetheless what is important to understand is the fact that, precisely through pushing forward a rhetoric that sees the adoption of such rules also vis-à-vis cyber operations, the US is trying to make it legal to adopt aggressive force in retaliation also against cyber attacks reaching a certain threshold, which remains of difficult definition.[233] More in detail, the US is pushing forward the notion of "equivalence", which states how against "a cyber attack [that] produces the death, damage, destruction or high-level disruption [equal to those] a

---

[230] White House, *International Strategy for Operating in Cyberspace. Prosperity, Security, and Openness in a Networked World*, 14.
[231] White House, *National Security Strategy*, 13
[232] Dunn Cavelty, "The Militarisation of Cyberspace", 148.
[233] Lewis, *Conflict and Negotiation in Cyberspace*, 39.

traditional military attack would cause, then it would be a candidate for a 'use of force' consideration, which could merit retaliation".[234]

7.1.2. Military

Regarding the documents published by the military, the 2004 NMS states that "[t]he Joint Force requires the ability to conduct information operations, including electronic warfare, computer network operations [and that] [i]nformation operations, both offensive and defensive, are key to ensuring US freedom of action across the battlespace".[235] Despite this passage not really fitting with any of the presented "offensiveness" sub-themes, it does display a strategic thinking tuned toward an aggressive usage of the cyber medium. In 2006, the NMS for Cyberspace Operations further pushed the discourse towards an ever more aggressive tone.[236] The sub-theme of domination can be found, as well as a signalling regarding the willingness to conduct offensive cyber operations. Four passages stand out: 1) "[T]he United States must have cyberspace superiority to ensure our freedom of action and deny the same to our adversaries through the integration of network defense, exploitation, and attack;[237] 2) "[o]ffensive capabilities in cyberspace offer the United States and our adversaries an opportunity to gain and maintain the initiative. DOD cyberspace operations

---

[234] Bouwmeester, Folmer, and Ducheine, "Cyber Security and Policy Responses", 28.
[235] Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2004* (Washington, DC, 2004), 18.
[236] Saltzman, "Cyber Posturing and the Offense-Defense Balance", 47.
[237] Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, 1.

are strongest when offensive and defensive capabilities are mutually supporting";[238] 3) "[DOD] will execute the full range of military operations […] in and through cyberspace to defeat, dissuade, and deter threats against US interests";[239] and 4) "cyberspace [should be used] to accelerate [the] decision-making cycle while degrading that of the adversary [as well as] exploiting adversary cyberspace vulnerabilities".[240]

Similarly to the 2004 one, despite not really having any discursive practices falling under a specific sub-theme, the 2011 NMS signals a readiness to act implementing the necessary resources to oppose "any nation's actions that jeopardize access to and use of […] cyberspace".[241]

A rhetoric further re-prised and taken up a scale, in line with the DOD's Cyber Strategy of the same year, as later shown, within the NMS published in 2015. Such a document indeed speaks of a willingness to "project power across all domains",[242] therefore also the cyber one, to defeat adversaries.[243]

7.2. Active Cyber Defence - a paradigm connoting an offensive strategic posture

This sub-chapter aims at further better clarifying why from a discursive thematic point of view the DOD's 2011 Strategy for Operating in

---

[238] Ibid., 10.
[239] Ibid., 2.
[240] Ibid., 19.
[241] Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2011,* 14.
[242] Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2015*, 11
[243] Ibid.

Cyberspace finds a place under both the "defensiveness" and "offensiveness" thematic categories. If, as seen such strategy contains mainly sub-themes/codes linked to "defensiveness", the reason why arguably also a degree of "offensiveness" is present lies in "active cyber defence" (ACD) measures. Indeed, such a term first appeared precisely in the 2011 DOD's strategy, discussed under the second of the five strategic initiatives highlighted in the document, the one titled "DoD will employ new defense operating concepts to protect DoD networks and systems".[244] According to the strategy, the DOD has been implanting new defensive paradigms in order to face the challenges deriving from an ever-increasing malicious cyber activity.[245] Despite not sharing too many technical and operational details on it, ACD are highlighted as being the new kind of defences to serve such purpose, defined as following: "DoD's synchronised real-time capabilities to discover, detect, analyze, and mitigate threats[,] [operating] at network speed using sensors, software and intelligence to detect and stop malicious activity ideally before it can affect DoD networks and systems".[246]

Leaving aside the broad discussions on both the legality and positive and negative consequences of ACD, the present chapter aims at unpacking such defensive paradigm and demonstrate how under certain aspects it is possible to assert how its implementation can be interpreted as a subtle manifestation of aggressiveness, hence proof of the fact that the US cyber strategic culture is being informed by a norm of offensiveness. The present

---

[244] Department of Defense, *Strategy for Operating in Cyberspace.*
[245] Ibid., 7.
[246] Ibid.; Rosenzweig, "International Law and Private Actor Active Cyber Defensive Measures", 105.

chapter is divided in three parts. Initially, a brief overview of ACD is presented in order to build the ground for further exploration. Secondly, the briefly previously introduced defensive conceptualisation of ACD is outlined. Thirdly, a more in depth analysis is undertaken, displaying how ACD also bears a more aggressive face.

7.2.1. A general overview

ACD since its first appearance on the DOD's 2011 Strategy for Operating in Cyberspace maintained an aura of ambiguity around itself, remaining "one of the most debated concepts in cybersecurity".[247] Scholars from various fields of study have been writing extensively on it. Indeed, a universally accepted conceptualisation seems to be lacking, not only among academics and experts, but also among international actors. For instance, whether debates are on-going in academia, such a situation has been observed also in international fora, such as NATO. [248]

In general terms, the debates on ACD have as central point of contention the broadness to be attributed to such defensive paradigm. As the remainder of the present chapter highlights, on one side there are those

[247] Paul Rosenzweig, Steven P. Bucci, and David Inserra, "Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense", *The Heritage Foundation*, No. 3188 (May 5, 2017), 1. Available at: https://www.heritage.org/sites/default/files/2017-05/BG3188.pdf.

[248] Joshua Keating, "U.S. and Europe at odds over cyberdefense policy?", *Foreign Policy*, October 5, 2010 (accessed June 2018), http://foreignpolicy.com/2010/10/05/u-s-and-europe-at-odds-over-cyberdefense-policy/.

who contend that ACD measures are to be understood as only those proactive steps taken within the victim's network; while on the other, there are those who argue that ACD is a much broader paradigm, encompassing also more aggressive measures, which go beyond the victim's network "boundaries". Nonetheless, point of contact among the debaters is the fact that ACD equals to proactiveness rather than simple reactiveness; or in other words, to measures that not simply wait passively, but that directly engage with the malicious actor/activity before and during the attack in more or less aggressive ways.[249]

7.2.2. Defensive ACD

Regarding the fist position, both Lee and Buchanan understand ACD as a set of measures to be applied within one owns networks in order to bolster overall defensive and resiliency capabilities. Lee parallels ACD to intelligence gathering and usage, crafting what he coins the "Active Cyber Defense Cycle". According to his view, ACD is to be understood as "the process of analysts monitoring for, responding to, learning from, and applying their knowledge to threats internal to the network".[250] Mirroring such an interpretation, Buchanan speaks of "hunting" as the proactive "look

---

[249] Irving Lachow, *Active Cyber Defense: A Framework for Policymakers* - Policy Brief (Washington DC: Center for North American Security, February, 2013), 1. Available at: https://s3.amazonaws.com/files.cnas.org/documents/CNAS_ActiveCyberDefense_Lachow_0.pdf?mtime=20160906080446.

[250] Robert M. Lee, *The Sliding Scale of Cyber Security* (SANS Institute, August, 2015), 9 - 15. Available at: https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240.

within the network for weaknesses and for malicious code that may have exploited […] weaknesses".[251]

Many techniques are highlighted as falling under the umbrella of the term "hunting", such as: 1) network security monitoring, a term that dates back to the early 2000s, which indicates "the collection, analysis and escalation of indications and warning to detect and respond to insertions";[252] 2) conducting memory forensics, "finding and extracting forensics artefacts from a computer's physical memory" in seeking the presence of malicious code;[253] and, 3) setting up some penetration testing to assess the strength of the defences.[254] Other specific measures fitting this conceptualisation of ACD are so-called "white worms", also known as "defense-ware".[255] On one hand, such benign software are programmed to identify and destroy malicious malware in an automated way,[256] and on the other to identify

---

[251] Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (Oxford University Press, 1st edition, February 1, 2017), 58.
[252] Richard Bejtlich, *The Practice of Network Security Monitoring: Understanding Incident Detection and Response* (No Starch Press, 2013), 1.
[253] Graham, Howard, and Olson, *Cyber Security Essentials*, 267; Michael Hale Ligh et al., *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac memory* (John Wiley & Sons, 2014).
[254] Sugandh Shah and B. M. Mehtre, "A Modern Approach to Cyber Security Analysis Using Vulnerability Assessment and Penetrating Testing", *International Journal of Electronics Communication and Computer Engineering*, Vol. 4, No. 6 (2013), 47 - 52; Anestis Bechtsoudis and Nicolas Sklavos, "Aiming at Higher Network Security through Extensive Penetration Tests", *IEEE Latin America Transactions,* Vol. 10, No. 3 (April, 2012), 1752 - 1756.
[255] Ren Zheng, Wenlian Lu, and Shouhuai Xu, "Active Cyber Defense Dynamics Exhibiting Rich Phenomena", in *Proceedings of the 2015 Symposium and Bootcamp on the Science of Security*, Article No. 2 (April, 2015).
[256] Ibid.

intrusion and carry out recovery procedures as well.[257] So-called "honeypots" also serve some of the above-mentioned purposes. Identified as a form of decoy, as their name suggest "honeypots" are information system resources that are designed to duplicate a valuable and potential target as closely as possible in order to lure and deceive attackers, being then able to collect precious data about the malicious activity and procedures, exposing also vulnerable services.[258] Indeed, their value rests in "the unauthorised or illicit use of that resource".[259] Finally, some experts enrich this particular notion of ACD stressing the fact that they serve the purpose of confounding and slowing down an attacker already within the system, rather than trying to block access in the first place.[260] One technique that long has been studied, tested, and applied is so-called "address hopping". Drawing insights from radio frequency communications, this technique grants the possibility to a computer's network to change identity in a dynamic way during the transmission of data.[261] In other words, "address hopping" can be

---

[257] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press, 2012), 108; Wenlian Lu, Shouhuai Xu, and Xinlei Yi, "Optimizing Active Cyber Defense", in *Proceedings of the 4th Conference on Decision and Game Theory for Security*, Vol. 8252 (2013), 206 - 225, 210.

[258] Kristin E. Heckman et al., *Cyber Denial, Deception and Counter Deception: A Framework for Supporting Active Cyber Defense* - Advances in Information Security (Book 64) (Springer, 2015), 73.

[259] Graham, Howard, and Olson, *Cyber Security Essentials*, 277.

[260] Fabio De Gaspari, Sushil Jajodia, Luigi V. Mancini, and Agostino Panico, "AHEAD: A New Architecture for Active Defense", *SafeConfig '16: Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense* (October 24, 2016), 11 - 16.

[261] Leyi Shi, et al., "Port and Address Hopping for Active Cyber-Defense", in *Intelligence and Security Informatics. PAISI 2007. Lecture Notes in Computer Science*, Vol. 4430, edited by Christopher C. Yang et al. (Springer, 2007), 295 - 300, 296.

understood as a form of obfuscation, which primary role is that of confusing the attacker.[262]

Former Deputy Secretary of Defense William J. Lynn III stressed the importance of building the capacity to "hunt" and attack directly on US network "to get the intruders who do get past the initial defenses".[263] From his words, it is possible to appreciate the fact that all the above-mentioned techniques, which are proactive but defensive (remaining within the victim's network boundaries), do fall under the DOD's definition of ACD measures. So under this light, it is possible to argue that, at least on the surface, DOD's conceptualisation of ACD is yes proactive but informed by a norm of "defensiveness", since the mentioned techniques all somewhat fall within the first, and arguably also second, sub-theme of such "thematic normative category".

7.2.3. Offensive ACD

As briefly introduced, within the literature there are also those who conceptualise ACD in a way diametrically opposite from that adopted by Lee and Buchanan. Many scholars indeed broaden the concept of ACD inserting within it also more aggressive cyber operations. For instance, Carr

---

[262] Keith A. Repik, *Defeating Adversary Network Intelligence Efforts with Active Cyber Defense Techniques* (DTIC Document, 2008), 22. Available at: http://www.dtic.mil/dtic/tr/fulltext/u2/a488411.pdf.

[263] Former Deputy Defense Secretary William J. Lynn III quoted in Jim Garamone, "Lynn Explains U.S. Cybersecurity Strategy", *DoD News*, September 15, 2010 (accessed June 2018), http://archive.defense.gov/news/newsarticle.aspx?id=60869.

defines ACD as also containing "electronic countermeasures designed to strike attacking computer systems and shut down cyber attacks midstream". [264] Accordingly, often it has been pointed out how ACD generally falls in either one of the following: "detection and forensics, deception, and attack termination".[265]

A recent study conducted by the World Economic Forum has stated that ACD as a term "captures a spectrum of proactive cybersecurity measures that fall between traditional passive defenses and offense".[266] Similarly, the George Washington University's Center for Cyber and Homeland Security published some graphics that by clarifying some of the techniques found along the mentioned spectrum highlights how vast the concept of ACD is, de-facto spanning from passive defence to cyber offense.[267]

Dewar, drawing from the DOD's definition and this aggressive version of ACD, offers a middle-ground definition of it, which builds a bridge between the two above mentioned. In his view, ACD is to be understood as a two-fold security paradigm employing "the real-time identification and

---

[264] Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (O'Reilly Media, 2010), 46.
[265] Lachow, *Active Cyber Defense: A Framework for Policymakers*, 5.
[266] Irving Lachow, "The promise and peril of active cyber defense", *The Hill*, April 18, 2018 (accessed June 2018), http://thehill.com/opinion/cybersecurity/383704-the-promise-and-peril-of-active-cyber-defense.
[267] Center for Cyber and Homeland Security - George Washington University, *Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats* (October, 2016), 10. Available at: https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf.

mitigation of threats [within] defenders' networks [and] the capacity to take aggressive, external, offensive countermeasures".[268] More in detail, ACD is "an approach to achieving cyber security predicated upon the deployment of measures to detect, analyse, identify and mitigate threats to and from communications systems and networks in real-time, combined with the capability and resources to take proactive or offensive action against threats and threat entities including action in those entities' home networks".[269]

Such more aggressive techniques said to fall within ACD are all some sorts of retaliatory countermeasures, which have been commonly labelled by experts as "hack back", a name that clearly connotes offensiveness, since it entails accessing the source of the attack, going beyond the victim's network "boundaries". Indeed, measures falling under the umbrella of "hack back" range from invasive techniques to various counterstrike methods all deployed to access the attacking source to either disable (disrupt), destroy, or seize control of it, using for example armed payloads.[270] Some examples are "botnet takedowns, white hat ransomware, [and] efforts to recover stolen data by [indeed] hacking back".[271]

---

[268] Dewar, "The Triptych of Cyber security", 10.
[269] Ibid.
[270] John Curry, "Active Defence", *ITNOW*, Vol. 54, No. 4 (December 1, 2012), 26 - 27; Emilio Iasiello, "Hacking back: not the right solution", *Parameters*, Vol. 44, No. 3 (Autumn, 2014), 105 - 113; Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option* (Rowman & Littlefield, 2017) [Kindle Edition], 177.
[271] Rosenzweig, Bucci, and Inserra, "Next Steps for U.S. Cybersecurity in the Trump Administration", 3.

Further, an aggressive understanding of ACD does not encompass just "hacking back" in the sense of going beyond one own's boundaries to aggressively target an adversary network or system to harm it, as in shutting it down or disrupting it. According to some, offensive/external ACD also means gathering of data and intelligence; precious information on other states' cyber capabilities and intrusion plans, which are then exploited to strengthen cyber defences.[272] Despite this view being shared by many within the literature, as already mentioned, this aggressive understanding of ACD as intelligence gathering is not taken into account.

At first glance, the definition of ACD given by the DOD does not lend itself easily to a more aggressive reading, however already by taking into consideration the technical debate on such defensive paradigm, which point out also their potential offensive conceptualisation, coupled with the mentioned "militarization" historical context characterised by other proofs of aggressive use of the cyber medium by the US, arguably their adoption signals a norm of "offensiveness".

In order to dive deeper into how ACD is conceptualised within the US governmental circles another primary document must be brought under scrutiny, namely the already mentioned Presidential Policy Directive No. 20 (PPD-20). Whether on the surface it does seem that ACD encompasses proactive measures falling under the umbrella of "hunting", which engage with the adversary within the victim's network "boundaries", a textual

[272] Buchanan, *The Cybersecurity Dilemma*, 64.

analysis of PPD-20 arguably reveals that at the federal level ACD is conceptualised as also being characterised by aggressive proactive measures, which share an extra-territoriality connotation;[273] thus, in line with its "expanded" conceptualisation.

The originally secretive PPD-20 published under the Obama administration, precisely in 2012, is a document containing directives about the conduct of cyber operations by federal government agencies, as well as by the military, which updates principles and processes of the US national cybersecurity policy.[274] Since its disclosure by the Edward Snowden's leaks,[275] PPD-20 has been deemed truly important by experts and commentators since not only it sheds more light on the way the US thinks regarding its cyber power, but especially because it outlines many definitions, such as that of "cyber effect", "network defence", "defensive cyber effects operations" (DCEOs), and "offensive cyber effects operations" (OCEOs), which help clarifying the nature of ACD.

Regarding "cyber effect", a rather straightforward definition is given, being understood as "the manipulation, disruption, denial, degradation, or destruction of computers, information or communication systems,

[273] Dewar, "The Triptych of Cyber security", 11 - 13.
[274] Barack Obama, *Presidential Policy Directive No. 20* (Washington DC, White House, 2012).
[275] Glenn Greenwald and Ewen MacAskill, "Obama orders US to draw up overseas target list for cyber-attacks", *The Guardian*, June 7, 2013 (accessed June 2018), https://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

networks, physical or virtual infrastructures controlled by computers or information systems, or information resident thereon".[276]

"Network defence" is understood as actions and the use of software "on a computer, network [...] by the owner or with [its] consent [...] for the primary purpose of protecting that computer, network, or system; data stored on, processed on, or transiting that computer, network, or system; or physical and virtual infrastructure controlled by that computer, network, or system".[277] A definition that seems to be close to the already mentioned conception of ACD, or at least that underlines actions taken within the boundaries of a network.

Of most importance to understand the broader nature of ACD, is the term "defensive cyber effect operations" (DCEOs), which defines all such activities, "other than network defence and cyber collection[,] that are intended to enable or produce cyber effects outside US Government networks for the purpose of defending or protecting against imminent threats or on going attacks or malicious cyber activity against US national interests from inside of outside cyberspace".[278]

According to Flowers and Zeadally, the fact that DCEOs share the purpose of defending and protecting US national interests, coupled with their semantically constructed differentiation from both network defence and

[276] Obama, *Presidential Policy Directive No. 20*, 2.
[277] Ibid.
[278] Ibid., 3.

cyber collection activities, means that DCEOs "can encompass a broad range of proactive activities [in line with their stated purpose] that can be used for pre-emptive or first-strike initiatives".[279]

Moreover, so-called "non-intrusive defensive countermeasures" (NCDMs), which are identified by PPD-20 as a subset of DCEOs and defined as including activities not requiring direct access to terminals and information on them without the consent of the owner, and creating only "the minimum cyber effects needed to mitigate the threat activity",[280] underline the presence of another non-identified category of DCEOs whose activity is far more severe than that of NCDMs.

Therefore, ACD can arguably be understood as such other subset of DCEOs.[281] In addition, more proof for such an interpretation can be gathered from the section "anticipatory action".[282] Within such portion of the directive, the reference to "anticipatory actions taken against imminent threats",[283] as included in DCEOs, further hints towards the point Flowers and Zeadally make.[284] Accordingly, the two academics offer a definition of ACD based on their analysis of PPD-20 as including "operations and related programs or activities conducted by or on behalf of the US Government,

---

[279] Angelyn Flowers and Sherali Zeadally, "US Policy on Active Cyber Defence", *Homeland Security & Emergency Management*, No. 11, Vol. 2 (2014), 289 - 308, 295.
[280] Obama, *Presidential Policy Directive No. 20*, 3.
[281] Flowers and Zeadally, "US Policy on Active Cyber Defence", 295.
[282] Obama, *Presidential Policy Directive No. 20*, 8.
[283] Ibid.
[284] Flowers and Zeadally, "US Policy on Active Cyber Defence", 297.

that manipulate, disrupt, deny, degrade, or destroy computers, information or communication systems, networks, physical or virtual infrastructures controlled by computers or information systems, or information resident thereon for the purpose of defending or protecting US national interests against immediate threats or on going attacks or malicious cyber activity occurring inside or outside cyberspace".[285]

Overall, given the language adopted within PPD-20 and the reference made to pre-emptive and first-strike options, it can be argued that such actions are closer to offense rather than simple defence, "rendering ACD a pseudonym for offensive cyber actions,[286] and those practices falling under the umbrella of "hack back". It does then seem that the US understands ACD in line with the mentioned definition offered by Dewar.

With this background in mind, arguably the signalling of the Pentagon of its implementation of ACD underlies a double rhetoric, both defensive and offensive. ACD, if intended in line with Dewar do seem to be a (ambiguous) vehicle showing how "offensiveness" is informing the US "cyber strategic culture", embodying two of its sub-themes, namely retaliation and preemption/prevention.

Finally, more insights do come the notion of Defensive Cyberspace Operations (DCOs). Through such kind of operations, which can be conducted in response to attacks of various intents, either exploitations or

[285] Ibid., 295.
[286] Ibid., 303.

actual damage, the military is called to defend the nation, or at least the assets assigned to it.[287] DCOs implement both passive and active cyberspace defence activities implemented to outmanoeuvre adversaries and "change the current paradigm where the attacker enjoys significant advantage";[288] DCOs can take place both within the owned networks' boundaries, as well as beyond them, taking respectively the form of Internal Defensive Measures (IDMs) and Response Actions (RAs).[289] Whether IDMs involve those measures and techniques that fall within the "hunting" paradigm, RAs involve more aggressive actions and countermeasures implemented directly against the "shooter".[290] Such a conceptualisation seems to be in line with the broader/extended conceptualisation of ACD presented in this chapter. Overall, arguably this is yet another proof that within the US ACD is conceptualised and implemented also in an aggressive way, being therefore a vehicle of the "offensiveness" norm informing the "cyber strategic culture".

7.3. The 2015 DOD's Cyber Strategy - "offensiveness" more openly manifested

In this chapter attention is posed on the Cyber Strategy published by the DOD during in April of 2015. Such official document offers yet other

---

[287] Jasper, *Strategic Cyber Deterrence,* 80.
[288] Major General Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Forces Quarterly*, No. 73, (2nd Quarter, 2014), 12 - 19, 15.
[289] Ibid., 16.
[290] These latter must be conducted in accordance with legal and policy guidelines. Jasper, *Strategic Cyber Deterrence*, 181.

glimpses into how the US military thinks of its cyber power. Such 33-page official document is an important discursive moment that demonstrates how the US "cyber strategic culture" is being informed by a norm of "offensiveness". Despite also elements connoting "defensiveness" are present, as previously pointed out, much emphasis is given to offensive cyber capabilities and their strategic use.[291] The present chapter aims at further unpacking the discourse found in the 2015 DOD Cyber Strategy. To do so some key passages of the text are presented and further explanation of the message they carry given.

During a speech at Stanford University in 2015, then US Secretary of Defense Ashton B. Carter set out the three missions CYBERCOM has in the cyber domain. According to his words, CYBERCOM mainly maintains a defensive role,[292] defending its own networks and weapons as well as helping defending the US from foreign cyberattacks; however, among such two mission, CYBERCOM also has that of providing offensive cyber options capable of enhancing the US military in a broader sense.[293]

---

[291] Danni Vinik, "America's secret arsenal", *Politico*, September 12, 2015 (accessed June 2018), https://www.politico.com/agenda/story/2015/12/defense-department-cyber-offense-strategy-000331.

[292] See the chapter on the Literature Review.

[293] Ashton Carter, "Remarks by Secretary Carter at the Drell Lecture, Cemex Auditorium, Stanford Graduate School of Business, Stanford, California", *U.S. Department of Defense*, April 23, 2015 (accessed June 2018), https://www.defense.gov/News/Transcripts/Transcript-View/Article/607043/remarks-by-secretary-carter-at-the-drell-lecture-cemex-auditorium-stanford-grad/.

Already from Mr Carter's words it is possible to grasp the fact that more openness has started to characterising the discourse around the possible use of cyber offensive capabilities. Further, his speech clearly signals the fact that, despite wishing to defend and deter cyber attacks, the US military is ready to act in an aggressive manner when deemed necessary.[294]

Despite leaving some key questions still unanswered, for the first time the 2015 DOD Cyber Strategy not only openly acknowledges that cyber offensive capabilities have been, and are being developed, but also clearly states that the US has the capability to strike adversaries' information systems, being ready to unleash its cyber arsenal under some circumstances.[295]

The document states the following: "[t]here may be times when the President or the Secretary of Defense may determine that it would be appropriate for the U.S. military to conduct cyber operations to disrupt an adversary's military-related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations".[296] And also the following: "[i]f directed, DOD should be able to use cyber operations to

---

[294] Herbert S. Lin, "Reflections on the New Department of Defense Cyber Strategy: What It Says, What It Doesn't Say", *Georgetown Journal of International Affairs*, Vol. 17, No. 3, (Fall/Winter, 2016), 5 - 13, 5.
[295] Henry Farrell, "What's new in the U.S. cyber strategy", *The Washington Post*, April 24, 2015 (accessed June 2018), https://www.washingtonpost.com/news/monkey-cage/wp/2015/04/24/whats-new-in-the-u-s-cyber-strategy/?noredirect=on&utm_term=.b04c45e07a4f.
[296] Department of Defense, *The DOD Cyber Strategy*, 5.

disrupt an adversary's command and control networks, military-related critical infrastructure, and weapons capabilities".[297]

The document thus arguably signals that the US thinks of its cyber arsenal also in offensive terms, as a proper "general-purpose war-fighting tool".[298] Precisely this rhetoric is what clearly distinguishes the 2015 document from its preceding ones, also more openly showing the norm of "offensiveness" being currently informing the US "cyber strategic culture".

For instance, a willingness to further integrate cyber operations into broader kinetic operational practices is clearly signalled within the document,[299] in showing how the cyber component of war will keep gaining momentum within the US "cyber strategic culture", thus arguably speeding up a process started already before the turn of the millennium, as pointed out in the chapter on the literature review.

Regarding preemption/prevention, the 2015 DOD document is rather clear on acting in an anticipatory self-defence way, stating that a possibility to act in a preemptive fashion exists also in cyberspace: "If directed by the President or the Secretary of Defense, the U.S. military may conduct cyber operations to counter an imminent or on-going attack against the U.S. homeland or U.S. interests in cyberspace. The purpose of such a defensive measure is to blunt an attack and prevent the destruction of property or the

[297] Ibid., 14.
[298] Ibid., 8.
[299] Ibid., 14.

loss of life".[300] Overall, speaking of offensive capabilities utilised under a defensive rubric is something usually captured under the paradigm of active defence,[301] thus arguably ACD. This passage shows that there is continuity within the DOD thinking, especially regarding the possibility to activate some offensive cyber capabilities to preempt an adversary operation. Thus, that the norm informing it did not really change in the time gap between the two cyber strategies, therefore between 2011 and 2015.

Linked to the possibility to act preventively is the bridge built by the strategy between cyber weapons and conflict escalation. The DOD utilises a discourse centred on its duty to provide the US President with several options to manage conflict escalation, one of them being its cyber capabilities. The fact that the strategy refers to periods of "heightened tensions",[302] which arguably precede a situation of open conflict, suggests how offensive cyber actions might be undertaken before the outbreak of hostilities, hence utilised early in a potential first strike.[303] This particular passage arguably also finds a link with ACD, or at least with those who have argued for a conceptualisation of it as also encompassing the usage of cyber weapons firstly for political reasons, as in the case of Stuxnet.[304]

---

[300] Ibid., 5.
[301] Lin, "Reflections on the New Department of Defense Cyber Strategy", 7.
[302] Department of Defense, *The DOD Cyber Strategy*, 14.
[303] Lin, "Reflections on the New Department of Defense Cyber Strategy", 8.
[304] Shane McGhee, Randy V. Sabett, and Anand Shah, "Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense", *Journal of Business & Technology Law*, Vol. 8, No. 1 (2013), 1 - 47, 12.

Finally, linked to all what said there is yet another discursive passage that demonstrates the presence of the sub-theme of domination and the practice of "operational preparation of the cyber battlefield" (OPB), therefore that the norm of "offensiveness" is informing the culture. Conducting active cyber reconnaissance and probing is rather ambiguous and not aggressive per se. In cyberspace, it is difficult to understand the purpose behind an operation since many of those tools utilised to simply surveil an adversary can be used to carry out more aggressive operations as well, ranging from intelligence collection to trapdoors and logic bombs placing. Nonetheless, with the discourse contained in the latest DOD strategy pointing out that cyber operations will be increasingly incorporated in the overall military power, that the DOD needs to provide the US President with a broad range of options in the moments possibly leading to an open conflict, and that preventive cyber strikes have been clearly signalled as a possible norm rather than exception, it is possible to argue that the US will likely carry on with continuity the practice of cyber OPB.[305] Regarding such practice, a recent article appeared on Nbc news underlined how (allegedly) the US already had violated some Russian critical infrastructure systems, achieving the possibility to take action against them. According to sources cited by the news article, the US military rigged Russian systems with trapdoors and logic bombs that could be activated in case of serious attacks, causing major disruption. A measure that the article parallels to that of "active defence",[306]

[305] Ibid.

[306] Ken Dilanian et al., "U.S. Govt. Hackers Ready to Hit Back If Russia Tries to Disrupt Election", *Nbc News*, November 5, 2016 (accessed June 2018), https://www.nbcnews.com/news/us-news/u-s-hackers-ready-hit-back-if-russia-disrupts-election-n677936.

and that somewhat confirms a more openly aggressive strategic posture adopted by the US towards its adversaries.[307]

7.4. The latest National Security Strategy - yet another step towards "offensiveness"

The National Security Strategy published at the end of 2017 has already been introduced. In the chapter explaining the predominance of the "defensiveness" thematic normative category the presence of the three sub-themes making up such theme's "story" have been showed. Here, the goal is to point out how the 2017 NSS also bears proof of the presence of the "thematic normative category" of "offensiveness". This official document contains some passages and expressions, which do point out a rather aggressive rhetoric, finding also a link with the discourse present within the 2015 DOD's Cyber Strategy and the analysed concept of ACD. The present brief chapter proceeds as following, firstly the general purpose of the discourse found in the 2017 NSS is presented; secondly, attention is posed to cybersecurity, with some key expressions and words being presented and analysed in building a bridge with the general purpose previously described, as well as with other empirical data coming from statements made by political and military officials.

[307] The fact that the article mentions specifically Russia is not random. Given the investigation and accusation against Russia's cyber-meddling campaign in the 2016 US presidential election, it does make sense that the US directs its aggressive signalling mainly towards her. Further, also in official strategic documents, Russia (alongside China and North Korea) is descried as a key adversary, as already briefly mentioned within the literature review.

From a general point of view, the latest NSS displays a rather aggressive rhetoric centred on a willingness to disrupt, defeat, and prevent activities that could endanger the US. In one key passage, the NSS states the importance and the need to "disrupt [and] defeat potential threats before they reach the United States".[308] The usage of "potential" as a pre-modifier well connotes the image of acting preemptively against menaces that still need to materialise, hence a predisposition or readiness to engage first, adopting a proactive aggressive defensive stance, rather than a simple reactive one. Such tone is the one to have in mind when also reading the passages devoted to cybersecurity, which to some extent directly mirror it.

For instance, the latest NSS states that the US "will go after […] digital networks […] of terrorists and criminals [who] evade detection",[309] "use sophisticated investigative tools to disrupt [illicit activities],[310] "impose […] costly consequences",[311] and "defeat [and go after] malicious actors",[312] be them terrorists, criminals, or state-actors. For example, recently the US has clearly stated to having conducted "cyber-campaigns" against assets pertaining to the infamous terrorist organisation known as Islamic State

[308] White House, *National Security Strategy of the United States of America*, 7.
[309] Eric Jensen, ""Risk Informed, But Not Risk Averse": the National Security Strategy Approach to Cyber Ops"*, Just Security*, December 22, 2017 (accessed June 2018), https://www.justsecurity.org/50066/risk-informed-risk-averse-national-security-strategy-approach-cyber-ops/.
[310] White House, *National Security Strategy of the United States of America*, 11.
[311] Ibid., 13.
[312] Ibid., 12, 4.

(IS). [313]

Further, in one of the most important passages for the analysis carried out in the present paper, the NSS states that in doing so the US will be "risk informed but not risk averse in considering [its] options".[314] An expression that seems not in line with the overall tone found in previous White House documents, which is characterised by a higher degree of prudence. For example, the 2011 Strategy for Operating in Cyberspace states that the US "will carefully weigh the costs and risks of action against the costs of inaction".[315]

According to some commentators, precisely the expressions, "go after", "impose costs", disrupt", "defeat" all are signs of the aggressiveness lying at the bottom of US cybersecurity discourse. Indeed, they participate in showing how the US "cyber strategic culture" is increasingly being informed by "offensiveness". Such a discourse connotes a more proactive and forward leaning strategic posture,[316] thus in line with what signalled in the 2015 DOD's Cyber Strategy, finding also a link with the analysed ACD (and DCO as well). Finally, the bold statement that the US will not be "risk averse", when evaluating its possible actions, entails the possibility to utilize the cyber arsenal, despite from a self-defence position, to conduct

[313] Jeppe Teglskov Jacobsen and Jens Ringsmose, "Cyber-bombing ISIS: why disclose what is better kept secret?", *Global Affairs*, Vol. 3, No. 2 (2017), 125 - 137.
[314] Ibid., 32.
[315] White House, *International Strategy for Operating in Cyberspace. Prosperity, Security, and Openness in a Networked World*, 14.
[316] Jensen, "Risk Informed, But Not Risk Averse".

first strike or retaliatory cyber operations. Therefore, also in the latest NSS the sub-themes of retaliation and preemption/prevention are present.

The overall tone found in the 2017 NSS seems to be in line with remarks made by President Trump during his presidential political campaign. In 2016, Mr Trump spoke of the need for the US to achieve the capacity to launch "crippling cyber counterattacks", and retain dominance in the cyber medium.[317] It must be noted that, already before Mr Trump's remarks, other top US officials invoked the need for more offensive cyber capabilities. Admiral Michael S. Rogers, former head of CYBERCOM and NSA, underlined the need to boost the military's overall cyber offensive capabilities to better deter threats and malicious actors. A position endorsed by both senators McCain and King and long advocated by former (and first) head of CYBERCOM General Keith Alexander.[318] Overall, it does indeed seem that the strategic thinking shared by such personalities is being reflected in official documents, which in turn demonstrate how the US "cyber strategic culture", despite displaying "defensiveness", is also being increasingly informed by "offensiveness".

---

[317] Aaron Boyd, "Trump administration promises more aggressive, less political cyber stance", *Federal Times*, November 9, 2016 (accessed June 2018), https://www.federaltimes.com/2016/11/09/trump-administration-promises-more-aggressive-less-political-cyber-stance/.

[318] Ellen Nakashima, "Cyber chief: Efforts to deter attacks against the U.S. are not working", *The Washington Post*, March 19, 2015 (accessed June 2018), https://www.washingtonpost.com/world/national-security/head-of-cyber-command-us-may-need-to-boost-offensive-cyber-powers/2015/03/19/1ad79a34-ce4e-11e4-a2a7-9517a3a70506_story.html?noredirect=on&utm_term=.76041a345dc9.

In the 1970s, Russell Frank Weigley clearly separated between military and national strategy. A division based on the differing ways through which goals are meant to be achieved. Whether militaries strive to achieve their goals by threat or use of force, civil governmental bodies focus on developing "political, economic, and psychological powers".[319] Despite such a dichotomy being fully present within the US cyber strategic culture, since it is indeed the military the body that has been demonstrating a tendency to prefer a display of force rather than the White House, with the 2017 NSS such a differentiation is starting to be eroded. If it is true that the process of militarisation present since the early 2000s has seen the military taking an increased role in defending the US in cyberspace, with an increasing recognition of such a role by civil governmental bodies, arguably within official documents prior to 2017 no such similarities in tone and rhetoric between the White House and Pentagon can be found. Something that further demonstrates how the overall US "cyber strategic culture" is developing a more aggressive rhetoric, being thus informed by a norm of "offensiveness".

[319] Russel Frank Weigley, *The American Way of War: A History of United States Military Strategy and Policy* (New York: Macmillan, 1973); Toje, "The EU Security Strategy Revised", 177.

8. Concluding remarks

8.1. Discussion and summary of findings

The present dissertation has sought to analyse the US approach to cybersecurity from a national strategic point of view, seeking to understand whether it displays more a defensive of aggressive posture, and whether it is possible to speak of a "shift", or at least track an evolution of it. The historical timeframe taken under scrutiny has been the one the world is currently undergoing, said to have begun in the early 2000s and labelled by experts as "militarization".

Overall, the literature already has provided some proofs of a "shift" towards an aggressive use of the cyber medium by the US during the 1990s and especially since the early 2000s. Precisely this rich literature has formed the starting point of the present dissertation, which however has intended to further expand the already formed knowledge, analysing and approaching more recent primary and secondary sources from a rather different theoretical perspective than those found within the literature on the topic. Indeed, the author has approached the US strategic behaviour from an ideational and interpretative point of view, focusing on the norms that seem to be informing and mirroring what has been called the US "cyber strategic culture".

Drawing insights from both the meta-theoretical tradition of Constructivism and from the research agenda of strategic culture studies, the present thesis has adopted a methodology centred on discourse, as well as on the analysis of themes, informed precisely by the mentioned theoretical approaches. Overall, two opposite "thematic normative categories" have been built, following an initial a-priori approach, deriving insights from the literature, then refined with the content found within the gathered and assessed primary sources. Their names reflect the kind of strategic behaviour and norms the author was interested in, respectively "defensiveness" and "offensiveness". In brief, "defensiveness" entails a research for security regarding threats and risks arising from cyberspace that not necessarily decreases that of other actors; while "offensiveness" is linked to a logic of zero-sum and notion of cyber war, entailing a more aggressive strategic behaviour centred around a potential use of force. The three sub-themes making up their respective "stories" reflect such conceptualisation, being for "defensiveness", network security/defence, cyber-resilience, and cooperation; while for "offensiveness": preemption/prevention, retaliation, and domination.

The methodology mentioned above has been applied to a set of official documents and texts, published by the White House and military, with attention being mostly directed towards the defensive paradigm of "active cyber defence" (ACD) measures, the 2015 Department of Defense's (DOD) Cyber Strategy, and latest 2017 White House's National Security Strategy (NSS).

Rather in line with what highlighted in the literature, the present thesis has uncovered that the norm of "defensiveness" has been predominantly and steadily informing the US "cyber strategic culture" during the scrutinised historical period. Indeed, all three sub-themes making up the "story" of "defensiveness" constantly re-appear throughout the assessed primary sources.

Regarding the other norm, that of "offensiveness", of most interest for the dissertation itself, a more complicate picture has been delineated. Indeed, whether some hints of it can be found within documents published before 2011, it is from that moment onward when arguably such a norm has been mainly informing/mirroring the US "cyber strategic culture".

Already in documents published in 2004 and 2006, the military has been displaying a rather aggressive rhetoric regarding the use of the cyber medium, something nonetheless in line with the information provided by the surveyed secondary literature, and already proofs of presence of the norm of "offensiveness" highlighted by the literature. Such a rhetoric can also somewhat be found in documents from 2011 and 2015 from both the White House and military; primary sources (different from those thoroughly taken as key empirical ones) that however already do fall within the time period when a sort of evolution regarding the norm of "offensiveness" can be appreciated, as the present thesis argues.

The author has further uncovered the workings of such social structure especially in the concept of ACD, firstly introduced in 2011. Such a paradigm from a technical point of view also encompasses measures that are linked to the "thematic normative category" of "defensiveness", with the official discourse surrounding it also hinting towards such norm;

nevertheless, by diving deeper in the ACD conceptualisation debate, the author has highlighted that a much broader understanding of it exists within the literature and among cybersecurity experts. ACD does indeed also encompass other type of measures and strategic behaviours that can be said to be closely linked and fall within the "offensiveness" theme. Further, the official document Presidential Policy Directive No. 20 (PPD-20), published in 2012 under the Obama administration, offers a more intimate look into how the US establishment conceptualises ACD, arguably as a paradigm encompassing also aggressive measures to be potentially projected towards adversaries. Overall, coupling the broader version of ACD, with its arguable understanding within the US shows how such defensive paradigm is a subtle vehicle showing that the US "cyber strategic culture" is informed by the norm of "offensiveness", displaying its sub-themes of retaliation and preemption/prevention.

Further, the 2015 DOD's Cyber Strategy, despite having some elements of "defensiveness" too, appears to openly acknowledge a more aggressive rhetoric. Within it, the discourse well points out two of the sub-themes making up the "story" of "offensiveness", namely preemption/prevention and domination, displaying also a link to ACD as well.

Finally, the latest NSS, contains the "offensiveness" sub-themes of retaliation and preemption/prevention, being characterised by a much bolder and aggressive rhetoric than precedent White House official documents, de-facto sharing a similar tone to the one present within military documents.

In conclusion, the present work somewhat has confirmed the thesis advanced by Saltzman on the fact that the US cyber strategic posture is of a "paradoxical defensive nature". The literature already has pointed out that the US, despite having demonstrated an actual aggressive use of the cyber medium, also behaved in restraint. The present analysis, has further uncovered how despite the discourse present in official strategies has been predominantly showing "defensiveness", since 2011 it is possible to speak of a "shift", or better, of an evolution with the discourse, despite being centred around a logic of self-defence, showing an increased presence of "offensiveness".

As a last remainder: what stated here must not be interpreted as encompassing causality, since such a claim was not one of the present research goals. Indeed, having uncovered the fact that the US "cyber strategic culture" seems to be increasingly informed by "offensiveness" does not necessarily entail that an aggressive strategic behaviour will be actually carried out. Indeed, the present thesis understands discourse and norms as social structures shaping a "realm of possibilities". Similarly, also the assessed official strategic documents signal potential behaviour, with states still left open to a different type of conduct.

8.2. Potential future research

Regarding the overall analysis of culture, the present thesis is just one initial step towards a much greater understanding of what here has been called the US "cyber strategic culture". More "intimate" empirical data is

needed to further study such a concept, which might become available in the near future, coupled with direct contacts with those directly involved in the decision-making process. Moreover, interesting would be to analyse whether the US strategic approach to cybersecurity reflects some much more consolidated and old cultural aspects such country has demonstrated also in other domains, conflict situations, technologies, and moments in history.

Overall, only mentioned in the present thesis, arguably the uncovered "offensiveness" finds a link with the logic of deterrence, which is the one that seems to predominate within the US establishment. Analysing whether there truly is a link between such an evolution and the logic of deterrence can well become the central topic of further research. Similarly, understanding all the driving forces and (geo)political and material factors behind such an increased preponderance of the norm of "offensiveness" through the adoption of various theoretical lenses also requires more research, posing focus to its interests and perceived constraint behaviour.

Finally, given the highly debated nature of ACD, much more research is needed on its conceptualisation and role within "cyber-inter-state" relationships. Indeed, whether some scholars argue in favour of the ethics of ACD,[320] others have pointed out some negative consequences its applicability might bring, especially regarding the international order, and Westphalian conception of sovereignty.[321] Because the analysis brought forward in the present thesis regards only the understanding and

[320] Dorothy E. Denning, "Framework and principles for active cyber defense", *Computer & Security,* Vol. 40 (February, 2014), 108 - 113.
[321] Betz and Stevens, *Cyberspace and the State*, Kindle Location 1201.

conceptualisation of ACD within the US, a broader research can result interesting, maybe comparing different states' conceptualisation and strategic approaches to it.

Bibliography

Aronson, Jodi. “A Pragmatic View of Thematic Analysis”, *The Qualitative Report*, Vol. 2, No. 1 (1995), 1- 3.

Ashford, Warwick. “UK leading in using red team cyber security testing”, *Computer Weekly*, March 31, 2017 (accessed June 2018), https://www.computerweekly.com/news/450416013/UK-leading-in-using-red-team-cyber-security-testing.

Ashford, Warwick. “Cooperation and exercises key to cyber defence, says Nato centre”, *Computer Weekly*, March 9, 2018 (accessed June 2018), https://www.computerweekly.com/news/252436575/Cooperation-and-exercises-key-to-cyber-defence-says-Nato-centre.

Attride-Stirling, Jennifer. ”Thematic networks: an analytic tool for qualitative research”, *Qualitative Research*, Vol. 1, No. 3 (2001), 385 - 405.

Barnard-Wills, David and Debi Ashenden. “Securing Virtual Space: Cyber War, Cyber Terror, and Risk”, *Space and Culture*, Vol. 15, No. 2 (2012), 110 - 123.

Barzashka, Ivanka.“Are Cyber-Weapons Effective?”, *The RUSI Journal*, Vol. 158, No. 2 (2013), 48 - 56.

BBC. “Edward Snowden: Timeline”, *BBC*, 20 August, 2013 (accessed May 2018), http://www.bbc.com/news/world-us-canada-23768248.

Beaumont, Peter. “US appoints first cyber warfare general”, *The Guardian*, May 23, 2010 (accessed May 2018),

https://www.theguardian.com/world/2010/may/23/us-appoints-cyber-warfare-general.

Bechtsoudis, Anestis and Nicolas Sklavos. "Aiming at Higher Network Security through Extensive Penetration Tests", *IEEE Latin America Transactions,* Vol. 10, No. 3 (April, 2012), 1752 - 1756.

Bejtlich, Richard. *The Practice of Network Security Monitoring: Understanding Incident Detection and Response* (No Starch Press, 2013).

Bendrath, Ralf. "The American Cyber-Angst and the Real World—Any Link?", in *Bombs and Bandwidth: The Emerging Relationship between Information Technology and Security,* edited by Robert Latham (New York: Free Press, 2003), 49 - 73.

Bendrath, Ralf. "The Cyberwar Debate: Perception and Politics in U.S. Critical Infrastructure Protection", in *The Internet and the Changing Face of International Relations and Security*, edited by Andreas Wenger, *Information & Security: An International Journal*, Vol. 7 (2001), 80 - 103.

Berg, Bruce L. *Qualitative Research for the Social Sciences* (Pearson, 4th edition, 2001).

Betz, David J. and Tim Stevens. *Cyberspace and the State: Toward a strategy for cyber-power* (Adelphi series Book 424; The International

Institute for Strategic Studies - IISS; Routledge; 1st edition, January 28, 2012) [Kindle Edition].

Biava, Alessia, Margriet Drent, and Graeme Herd. "Characterizing the European Union's Strategic Culture: An Analytical Framework", *Journal of Common Market Studies*, Vol. 49, No. 6 (2011), 1227 - 1248.

Bloomfield, Alan. "Time to Move On: Reconceptualizing the Strategic Culture Debate", *Contemporary Security Policy*, Vol. 33, No. 3 (2012), 437 - 461.

Bourne, Mike. *Understanding Security* (Palgrave, 2014 edition).

Bouwmeester, Han, Hans Folmer & Paul Ducheine. "Cyber Security and Policy Responses", in *Cyber Warfare: Critical Perspectives*, edited by Paul Ducheine, Frans Osinga, and Joseph Soeters (t.m.c. Asser press, 2012), 19 - 48.

Boyatzis, Richard E. *Transforming Qualitative Information: Thematic Analysis and Code Development* (SAGE Publications, Inc, 1st edition, April 16, 1998).

Boyd, Aaron. "Trump administration promises more aggressive, less political cyber stance", *Federal Times*, November 9, 2016 (accessed June 2018), https://www.federaltimes.com/2016/11/09/trump-administration-promises-more-aggressive-less-political-cyber-stance/.

Braun, Virginia and Victoria Clarke. “Using thematic analysis in psychology”, *Qualitative Research in Psychology*, Vol. 3, No. 2. (2006), 77 - 101, 79.

Braun, Virginia and Victoria Clarke. *Successful qualitative research: A practical guide for beginners* (SAGE Publications Ltd, 1st edition, April 5, 2013).

Brito, Jerry and Tate Watkins. “Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy”, *Harvard National Security Journal*, Vol. 3, No. 1 (2011), 39 - 84.

Bryant, Lt Col William D. (USAF). “Cyberspace Superiority: A Conceptual Model”, *Air & Space Power Journal*, Vol. 6, No. 6 (November–December, 2013), 25 - 44.

Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (Oxford University Press, 1st edition, February 1, 2017).

Bulletin of the Atomic Scientists. “Ronald Deibert: Tracking the emerging arms race in cyberspace”, *Bulletin of the Atomic Scientists*, Vol. 67, No. 1 (2011), 1 - 8.

Bulmer, Martin. “Concepts in the analysis of qualitative data”, *Sociological Review*, Vol. 27, No. 4 (1979), 651 - 677.

Buzan, Barry and Lene Hansen. *The Evolution of International Security Studies* (Cambridge University Press, 2009).

Carr, Jeffrey. "The Misunderstood Acronym: Why Cyber Weapons Aren't WMD", *Bulletin of the Atomic Scientists*, Vol. 69, No. 5 (2013), 32 – 37.

Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld* (O'Reilly Media, 2010).

Carr, Madeline. "Public–private partnerships in national cyber-security strategies", *International Affairs*, Vol. 92, No. 1 (2016), 43 - 62.

Carter, Ashton. "Remarks by Secretary Carter at the Drell Lecture, Cemex Auditorium, Stanford Graduate School of Business, Stanford, California", *U.S. Department of Defense*, April 23, 2015 (accessed June 2018), https://www.defense.gov/News/Transcripts/Transcript-View/Article/607043/remarks-by-secretary-carter-at-the-drell-lecture-cemex-auditorium-stanford-grad/.

Cavelty Dunn, Myriam. *Cyber-Security and Threat Politics: USA Efforts to Secure the Information Age* (New York: Routledge, 2007).

Cavelty Dunn, Myriam. "Cyber-Terror - Looming Threat or Phantom Menace?: The Framing of the US Cyber-Threat Debate", *Journal of Information Technology & Politics*, Vol. 4, No. 1 (2008), 19 - 36.

Cavelty Dunn, Myriam. “Like a phoenix from the ashes: The reinvention of critical infrastructure protection as distributed security”, in *Securing 'the Homeland': Critical Infrastructure, Risk and (In) Security*, edited by Myriam Dunn Cavelty and Kristian Søby Kristensen (Routledge, 1st edition June 18, 2008), 40 - 62.

Cavelty Dunn, Myriam and Manuel Suter. “Public-Private Partnerships are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection”, *International Journal of Critical Infrastructure Protection*, Vol. 4, No. 2 (2009), 179 - 187.

Cavelty Dunn, Myriam. “The militarisation of cyber security as a source of global tension”, in *Strategic Trends 2012: Key Developments in Global Affairs*, edited by Daniel Möckli (Center for Security Studies ETH Zurich, 2012), 103 - 124.

Cavelty Dunn, Myriam. “The Militarisation of Cyberspace: Why Less May Be Better”, in *2012 4th International Conference on Cyber Conflict*, edited by C. Czosseck, R. Ottis, and K. Ziolkowski (Talinn, Estonia: NATO CCD COE Publications, 2012), 141 - 153.

Cavelty Dunn, Myriam. “From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse”, *International Studies* Review, Vol. 15, No. 1 (2013), 105 - 122.

Cavelty Dunn, Myriam. "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities", *Science and Engineering Ethics*, Vol. 20, No. 3 (September 2014), 701 - 715.

Cavelty Dunn, Myriam, Mareile Kaufmann, and Kristian Søby Kristensen. "Resilience and (in)security: Practices, subjects, temporalities", *Security Dialogue*, Vol. 46, No. 1 (2015), 3 - 14.

Center for Cyber and Homeland Security - George Washington University. *Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats* (October, 2016). Available at: https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf.

Chen, Thomas M. *An assessment of the Department of Defense Strategy for Operating in Cyberspace* - The Letort Papers (Strategic Studies Institute and U.S. Army War College Press, 2013).

Cisco. *Cyber Resilience: Safeguarding the Digital Organization* (2016). Available at: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cyber-resilience-safeguarding-digital-org-wp.pdf.

Clarke, Richard A. and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It* (Ecco; Reprint edition, August 5, 2011).

Cole, Eric. *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization* (Syngress, 2012).

Creswellm John W. *Research design: Qualitative, quantitative, and mixed methods approaches* (SAGE Publications, Inc, 3rd edition, July 15, 2008).

Curry, John. "Active Defence", *ITNOW*, Vol. 54, No. 4 (December 1, 2012), 26 - 27.

De Gaspari, Fabio, Sushil Jajodia, Luigi V. Mancini, and Agostino Panico. "AHEAD: A New Architecture for Active Defense", *SafeConfig '16: Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense* (October 24, 2016), 11 - 16.

Deibert, Ronald J. and Rafal Rohozinski. "Risking Security: Policies and Paradoxes of Cyberspace Security", *International Political Sociology*, Vol. 4, No. 1 (March, 2010), 15 - 32.

Denning, Dorothy E. "Framework and principles for active cyber defense", *Computer & Security,* Vol. 40 (February, 2014), 108 - 113.

Department of Defense. *The Department of Defense Strategy for Operating in Cyberspace* (Washington, DC, July, 2011).

Department of Defense. *The DOD Cyber Strategy* (April, 2015).

DeSantis, Lydia and Doris Noel Ugarriza. "The Concept of Theme as Used in Qualitative Nursing Research", *Western Journal of Nursing Research*, Vol. 22, No. 2 (2000), 351 - 372.

Determann, Lothar and Karl-Theodor zu Guttenberg. "Spies Will Be Spies in War, Peace and Cyberspace", *Huffington Post*, September 13, 2014 (accessed June 2018), https://www.huffingtonpost.com/lothar-determann/cyberspace-spies_b_5583006.html?guccounter=1.

Dewar, Robert S. "The Triptych of Cyber security: a classification for active cyber defence", in *2014 6th International Conference on Cyber Conflict: Proceeding*, edited by P. Brangetto, M. Maybaum, J. Stinissen (NATO CCD COE Publications, 2014), 7 - 22.

Dilanian, Ken et al. "U.S. Govt. Hackers Ready to Hit Back If Russia Tries to Disrupt Election", *Nbc News*, November 5, 2016 (accessed June 2018), https://www.nbcnews.com/news/us-news/u-s-hackers-ready-hit-back-if-russia-disrupts-election-n677936.

Dinniss, Heather Harrison. *Cyber Warfare and the Laws of War* (Cambridge University Press, 2012).

Dobrygowski, Daniel. "Cyber resilience: everything you (really) need to know", *World Economic Forum*, July 8, 2016 (accessed June 2018),

https://www.weforum.org/agenda/2016/07/cyber-resilience-what-to-know/.

Domingo, Francis C. "China's Engagement in Cyberspace", *Journal of Asian Security*, Vol. 3, No. 2 (2016), 245 - 259.

Dunne, Tim, Milja Kurki, and Steve Smith. *International Relations Theories* (Oxford University, 2013).

Eberle, Christopher J. "Just War and Cyberwar, *Journal of Military Ethics*, Vol. 12, No. 1 (2013), 54 - 67.

ENISA. *Cybersecurity cooperation: Defending the digital frontline* (October 2013), available at: https://www.google.cz/search?q=cooperation+is+key+cybersecurity&oq=cooperation+is+key+cybersecurity&aqs=chrome..69i57.4646j1j7&sourceid=chrome&ie=UTF-8#.

Eriksson, Johan and Giampiero Giacomello. "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?", *International Political Science Review*, Vol. 27, No. 3 (July, 2006), 221 - 244.

Eriksson, Johan and Giampiero Giacomello, Eds. *International Relations and Security in the Digital Age* (London: Routledge, 2007).

Farrell, Henry. "What's new in the U.S. cyber strategy", *The Washington Post*, April 24, 2015 (accessed June 2018), https://www.washingtonpost.com/news/monkey-cage/wp/2015/04/24/whats-new-in-the-u-s-cyber-strategy/?noredirect=on&utm_term=.b04c45e07a4f.

Farrell, Theo. "Constructivist Security Studies: Portrait of a Research Program", *International Studies Review,* Vol. 4, No. 1 (Spring, 2002), 49 - 72.

Farwell, James P. and Rafal Rohozinski. "The New Reality of Cyber War", *Survival*, Vol. 54, No. 4 (2012), 107 - 120.

Finnemore, Martha and Kathryn Sikkin. International Norm Dynamics and Political Change, *International Organization*, Vol. 52, No. 4 (Autumn, 1998), 887 - 917.

Finnemore, Martha and Kathryn Sikkink. "TAKING STOCK: The Constructivist Research Program in International Relations and Comparative Politic", *Annual Review of Political Science*, Vol. 4 (June, 2001), 391 - 416.

Flowers, Angelyn and Sherali Zeadally. "US Policy on Active Cyber Defence", *Homeland Security & Emergency Management*, No. 11, Vol. 2 (2014), 289 - 308.

Friedberg, Ivo, Florian Skopik, Giuseppe Settanni, and Roman Fiedler. "Combating advanced persistent threats: From network event correlation to incident detection", *Computers & Security*, Vol. 48 (February, 2015), 35 - 57.

Galinec, Darko, Darko Možnik, and Boris Guberina. "Cybersecurity and cyber defence: national level strategic approach", *Automatika*, Vol. 58, No. 3 (2017), 273 - 286.

Garamone, Jim. "Lynn Explains U.S. Cybersecurity Strategy", *DoD News*, September 15, 2010 (accessed June 2018), http://archive.defense.gov/news/newsarticle.aspx?id=60869.

Gjelten, Tom. "First Strike: US Cyber Warriors Seize the Offensive", *World Affairs*, January/February 2013 (accessed June 2018), http://www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive.

Gomez, Miguel Alberto N. "Arming Cyberspace: The Militarization of a Virtual Domain", *Global Security and Intelligence Studies*, Vol. 1, No. 2 (Spring, 2016), 42 - 65.

Graham, James, Richard Howard, and Ryan Olson. *Cyber Security Essentials* (Auerbach Publications, 2011).

Gray, Colin. "Strategic Culture as Context: The First Generation of Theory Strikes Back", *Review of International Studies*, Vol. 25, No. 1 (1999), 49 - 69.

Gray, Colin S. *The Implication of Preemptive and Preventive War Doctrines: A Reconsideration* (Strategic Studies Institute, US Army War College, July, 2007).

Greenwald, Glenn and Ewen MacAskill. "Obama orders US to draw up overseas target list for cyber-attacks", *The Guardian*, June 7, 2013 (accessed June 2018), https://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

Haizler, Omry. "The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking", *Cyber, Intelligence, and Security*, Vol. 1, No.1 (January, 2017), 31 - 45.

Hansen, Lene and Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly*, Vol. 53, No. 4 (2009), 1155 - 1175.

Healey, Jason and Karl Grindal, Eds. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Cyber Conflict Studies Association, 2013).

Heckman, Kristin E. et al. *Cyber Denial, Deception and Counter Deception: A Framework for Supporting Active Cyber Defense* - Advances in Information Security (Book 64) (Springer, 2015).

Herzogm Christian, Christian Handke, and Erik Hitters. "Thematical Analysis of Policy Data", in T*he Palgrave Handbook of Methods for Media Policy Research*, edited by Van den Bulck, H, Puppis, M., Donders, K. & Van Audenhove, L (Basingstoke: Palgrave Macmillan, forthcoming). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3068081.

Hurd, Ian. "Constructivism", in *The Oxford Handbook of International Relations*, edited by Christian Reus-Smit and Duncan Snidal (Oxford University Press Inc., 2010), 298 - 316.

Hurwitz, Roger. "A New Normal? The Cultivation of Global Norms as Part of a Cybersecurity Strategy", in *Conflict and Cooperation in Cyberspace The Challenge to National Security*, edited by Panayotis A. Yannakogeorgos and Adam B. Lowther (Taylor & Francis, 2014), 233 - 264.

Iasiello, Emilio. "Hacking back: not the right solution", *Parameters*, Vol. 44, No. 3 (Autumn, 2014), 105 - 113.

Iasiello, Emilio. "What Happens If Cyber Norms Are Agreed To?", *Georgetown Journal of International Affairs*, Vol. 17, No. 3 (Fall/Winter, 2016), 30 - 37.

Jackson, Robert and Georg Sørensen. *Introduction to International Relations: Theories and Approaches* (Oxford University Press, 4th edition, April 19, 2010).

Jasper, Scott. *Strategic Cyber Deterrence: The Active Cyber Defense Option* (Rowman & Littlefield, 2017) [Kindle Edition].

Jensen, Eric. ""Risk Informed, But Not Risk Averse": the National Security Strategy Approach to Cyber Ops"*, Just Security*, December 22, 2017 (accessed June 2018), https://www.justsecurity.org/50066/risk-informed-risk-averse-national-security-strategy-approach-cyber-ops/.

Jepperson, Ronald L., Alexander Wendt, and Peter J. Katzenstein. "Norms, Identity, and Culture in National Security", in *The Culture of National Security: Norms and Identity in World Politics*, edited by Peter J. Katzenstein (New York: Columbia University Press, 1996), 33 - 75.

Johnston, Alastair Iain. *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History* (Princeton: Princeton University Press, 1995).

Joint Chiefs of Staff. *The National Military Strategy of the United States of America 2004* (Washington, DC, 2004).

Joint Chiefs of Staff. *The National Military Strategy for Cyberspace Operations* (Washington, DC, December, 2006).

Joint Chiefs of Staff. *The National Military Strategy of the United States of America 2011* (Washington, DC, February 8, 2011).

Joint Chiefs of Staff. *The National Military Strategy of the United States of America 2015* (Washington, DC, June, 2015).

Kallender, Paul & Christopher W. Hughes. "Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace", *Journal of Strategic Studies*, Vol. 40, No. 1-2 (2017), 118 - 145.

Katzenstein, Peter J. "Introduction: Alternative Perspectives on National Security", in *The Culture of National Security: Norms and Identity in World Politics*, edited by Peter J. Katzenstein (New York: Columbia University Press, 1996), 1 - 32.

Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", *International Security*, Vol. 38, No. 2, (Fall, 2013), 7 - 40.

Klein, Yithzak. "A theory of strategic culture", *Comparative Strategy*, Vol. 10, No. 1 (1991), 3 - 23.

Klohs, Julia and Arne Niemann. "Comparing the US National Security Strategy and the European Security Strategy in the first decade of the 21st century: converging but still different", *Mainz Papers on International and European Politics (MPIEP),* No. 8 (2014).

Kotler, Itzik. "The Key To Cybersecurity: Shared Intelligence And Industry Cooperation", *Forbes*, February 11, 2017 (accessed June 2018), https://www.forbes.com/sites/forbestechcouncil/2017/02/15/the-key-to-cybersecurity-shared-intelligence-and-industry-cooperation/#3ecb5e2c7eb8.

Krepinevich, Andrew F. "Cavalry to computer; the pattern of military revolutions", *The National Interest*, Vol. 37 (Fall, 1994), 30+.

Labaka, Leire, Josune Hernantes, and Jose M. Sarriegi. "A holistic framework for building critical infrastructure resilience", *Technological Forecasting & Social Change*, Vol. 103 (2016), 21 - 33.

Lachow, Irving. *Active Cyber Defense: A Framework for Policymakers* - Policy Brief (Washington DC: Center for North American Security, February, 2013). Available at: https://s3.amazonaws.com/files.cnas.org/documents/CNAS_ActiveCyberDefense_Lachow_0.pdf?mtime=20160906080446.

Lachow, Irving. "The promise and peril of active cyber defense", *The Hill*, April 18, 2018 (accessed June 2018), http://thehill.com/opinion/cybersecurity/383704-the-promise-and-peril-of-active-cyber-defense.

Lamont, Christopher. *Research Methods in International Relations* (SAGE Publications Ltd, 1st edition, May 20, 2015) [Kindle Edition].

Lange, Katie. "Cybercom Becomes DoD's 10th Unified Combatant Command", *DoDLive*, May 3, 2018 (accessed June 2018), http://www.dodlive.mil/2018/05/03/cybercom-to-become-dods-10th-unified-combatant-command/.

Lantis, Jeffrey S. "Strategic Culture: From Clausewitz to Constructivism", in *Strategic Culture and Weapons of Mass Destruction: Culturally Based Insights Into Comparative National Security Policymaking*, edited by Jeannie L. Johnson, Kerry M. Kartchner, and Jeffrey A. Larsen (Palgrave Macmillan, 2009), 33 - 54.

Lauterbach, Toby. ""Constructivism, Strategic Culture, and the Iraq War", *ASPJ Africa & Francophonie*, Vol. 2, No. 4 (4th Quarter, 2011), 61 - 92.

Laver, Harry S. "Preemption and the Evolution of America's Strategic Defense", *Parameters*, Vol. 35, No. 2 (Summer, 2005), 107 - 120.

Lawson, Sean. "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats", *Journal of Information Technology & Politics*, Vol. 10, No. 1 (2013), 86 - 103.

Lee, Robert M. *The Sliding Scale of Cyber Security* (SANS Institute, August, 2015). Available at: https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240.

Levy, Jack S. "Preventive War and Democratic Politics", *International Studies Quarterly*, Vol. 52, No. 1 (March, 2008), 1 - 24.

Lewis, James A. *Conflict and Negotiation in Cyberspace* (Center for Strategic & International Studies, February, 2013).

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge University Press, 2007).

Libicki, Martin C. *Cyberdeterrence and Cyberwar* (Santa Monica, RAND, 2009).

Libicki, Martin C. "Sub Rosa Cyber War", in *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by C. Czosseck and K. Geers (IOS Press, 2009), 53 - 87.

Liff, Adam P. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War", *Journal of Strategic Studies,* Vol. 35, No. 3 (2012), 401 - 428.

Ligh, Michael Hale et al. *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac memory* (John Wiley & Sons, 2014).

Lin, Herbert S. "Reflections on the New Department of Defense Cyber Strategy: What It Says, What It Doesn't Say", *Georgetown Journal of International Affairs*, Vol. 17, No. 3, (Fall/Winter, 2016), 5 - 13.

Linkov, Igor et al. "Resilience metrics for cyber systems", *Environ Syst Decis,* Vol. 33 (2013), 471 - 476.

Lock, Edward. "Refining strategic culture: Return of the second generation", *Review of International Studies*, Vol, 36, No. 3 (2010), 685 - 708.

Lock, Edward. "Strategic Culture Theory: What, Why, and How", *Oxford Research Encyclopedia of Politics,* September 26, 2017 (accessed May 2018), http://politics.oxfordre.com/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-320.

Lu, Wenlian, Shouhuai Xu, and Xinlei Yi. "Optimizing Active Cyber Defense", in *Proceedings of the 4th Conference on Decision and Game Theory for Security*, Vol. 8252 (2013), 206 - 225.

Matania, Eviatar, Lior Yoffe, and Michael Mashkautsan. “A Three-Layer Framework for a Comprehensive National Cyber-security Strategy”, *Georgetown Journal of International Affairs*, Vol. 17, No. 3 (Fall/Winter, 2016), 77 - 84.

Maurer, Tim. *Cyber norm emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber-security* (Discussion Paper #2011-11 Explorations in Cyber International Relations Discussion Paper Series Belfer Center for Science and International Affairs, 2011).

Mazanec, Brian M. *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons* (Potomac Books, November 1, 2015).

McGhee, Shane, Randy V. Sabett, and Anand Shah. “Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense”, *Journal of Business & Technology Law*, Vol. 8, No. 1 (2013), 1 - 47.

Mendell, Ronald. “Advanced persistent threat” (APT), *Encyclopædia Britannica Inc.*, December 10, 2015 (accessed March 2018), https://www.britannica.com/topic/advanced-persistent-threat.

Merriam-Webster. “Offense”, *Merriam-Webster,* (accessed June 2018), https://www.merriam-webster.com/dictionary/offense.

Merriam-Webster. n.d., “Discourse”, *Merriam-Webster.com*, last updated May 12, 2018 (accessed May 2018), https://www.merriam-webster.com/dictionary/discourse.

Meyer, Christoph O. "Convergence Towards a European Strategic Culture? A Constructivist Framework for Explaining Changing Norms”, *European Journal of International Relations*, Vol. 11, No. 4 (2005), 523 - 549.

Milliken, Jennifer. “The Study of Discourse in International Relations: A Critique of Research and Methods”, *European Journal of International Relations*, Vol. 5, No. 2 (1999), 225 - 254.

Moravcsik, Andrew. “Active Citation: A Precondition for Replicable Qualitative Research”, *Political Science and Politics*, Vol. 43, No. 1 (January, 2010), 29 - 35.

Mueller, Karl P. et al. *Striking First: Preemptive and Preventive Attack in U.S. National Security Policy* (RAND, 2006).

Myauo, Michele. “The U.S. Department of Defense Cyber Strategy: A Call to Action for Partnership”, *Georgetown Journal of International Affairs*, Vol. 17, No. 3, (Fall/Winter, 2016), 21 - 29.

Nakashima, Ellen. “Cyber chief: Efforts to deter attacks against the U.S. are not working”, *The Washington Post*, March 19, 2015 (accessed June 2018), https://www.washingtonpost.com/world/national-security/head-of-cyber-

command-us-may-need-to-boost-offensive-cyber-powers/2015/03/19/1ad79a34-ce4e-11e4-a2a7-9517a3a70506_story.html?noredirect=on&utm_term=.76041a345dc9.

Northcutt, Stephen. "Security Laboratory: Methods of Attack Series", *SANS*, May 2, 2007 (accessed June 2018), https://www.sans.edu/cyber-research/security-laboratory/article/log-bmb-trp-door.

Nowell, Lorelli S., et al. "Thematic Analysis: Striving to Meet the Trustworthiness Criteria", *International Journal of Qualitative Methods*, Vol. 16 (2017), 1 - 13.

Nye Jr., Joseph S. "Deterrence and Dissuasion in Cyberspace", *International Security*, Vol. 41, No. 3 (Winter, 2016/2017), 44 - 71.

O'Hanlon, Michael E. et al. "The New National Security Strategy and Preemption", *The Brookings Institution - Policy Brief*, No. 113 (December, 2002). Available at: https://www.brookings.edu/wp-content/uploads/2016/06/pb113.pdf.

Obama, Barack. *Presidential Policy Directive No. 20* (Washington DC, White House, 2012).

Olcott, Jake. "Cybersecurity Vs. Cyber Resilience", *Bit Sight*, December 7, 2017 (accessed June 2018), https://www.bitsighttech.com/blog/cyber-resilience.

Onuf, Nicolas. *World of Our Making: Rules and Rule in Social Theory and International Relations* (Routledge, 2012).

Pernik, Piret et al. National Cyber Security Organisation: United States (Tallinn, NATO CCD COE, 2016). Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf.

Repik, Keith A. *Defeating Adversary Network Intelligence Efforts with Active Cyber Defense Techniques* (DTIC Document, 2008). Available at: http://www.dtic.mil/dtic/tr/fulltext/u2/a488411.pdf.

Reus-Smit, Christian. "Constructivism", in *Theories of International Relations*, edited by Scott Burchill et al. (Palgrave Macmillan, 3rd edition, 2005), 188 - 212.

Rid, Thomas & Peter McBurney. "Cyber-Weapons", *The RUSI Journal*, Vol. 157, No. 1 (2012), 6 - 13.

Rosenzweig, Paul. "International Law and Private Actor Active Cyber Defensive Measures", *Stanford Journal of International Law*, Vol. 50, No. 1 (Winter, 2014), 103 - 118.

Rosenzweig, Paul, Steven P. Bucci, and David Inserra. "Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense", *The*

Heritage Foundation, No. 3188 (May 5, 2017). Available at: https://www.heritage.org/sites/default/files/2017-05/BG3188.pdf.

Ryan, Gery W. and H. Russel Bernard. "Techniques to Identify Themes", *Field Methods*, Vol. 15, No. 1 (February, 2003), 85 - 109.

Saltzman, Ilai. "Cyber Posturing and the Offense-Defense Balance", *Contemporary Security Policy*, Vol. 34, No. 1 (2013), 40 - 63.

Särelä, Mikko et al. "Evaluating intrusion prevention systems with evasions", *International Journal of Communication Systems*, Vol. 30, No. 6 (November, 2017).

Shachtman, Noah. "'Degrade, Disrupt, Deceive': U.S. Talks Openly About Hacking Foes", *Wired*, August 28, 2012 (accessed June 2018), https://www.wired.com/2012/08/degrade-disrupt-deceive/.

Shachtman, Noah. "Darpa Looks to Make Cyberwar Routine with Secret 'Plan X'", *Wired*, August 21, 2012 (accessed June 2018), https://www.wired.com/2012/08/plan-x/.

Shah, Sugandh and B. M. Mehtre. "A Modern Approach to Cyber Security Analysis Using Vulnerability Assessment and Penetrating Testing", *International Journal of Electronics Communication and Computer Engineering*, Vol. 4, No. 6 (2013).

Sharma, Amit. “Cyber Wars: A Paradigm Shift from Means to Ends”, *Strategic Analysis*, Vol. 34, No. 1 (2010), 62 - 73.

Sheldon, John B. “Deciphering Cyberpower: Strategic Purpose in Peace and War”, *Strategic Studies Quarterly*, Vol. 5, No. 2 (Summer, 2011), 95 - 112.

Shenk, Jerry. “Layered Security: Why It Works”, *SANS Institute* (2013). Available at: https://www.sans.org/reading-room/whitepapers/analyst/layered-security-works-34805.

Shi, Leyi, et al. “Port and Address Hopping for Active Cyber-Defense”, in *Intelligence and Security Informatics*. *PAISI 2007. Lecture Notes in Computer Science*, Vol. 4430, edited by Christopher C. Yang et al. (Springer, 2007), 295 - 300.

Singer, P. W. and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know®* (Oxford University Press, 1st edition, January 3, 2014).

Slayton, Rebecca. “What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment”, *International Security*, Vol. 41, No. 3, (Winter, 2016/2017), 72 - 109.

Snyder, Jack. *The Soviet Strategic Culture: Implications for Limited Nuclear Operations* (Santa Monica: RAND, 1977).

Stevens, Tim. “A Cyberwar of Ideas? Deterrence and Norms in Cyberspace”, *Contemporary Security Policy*, Vol. 33, No. 1 (April, 2012). 148 - 170.

Stevens, Tim. “Apocalyptic Visions: Cyber War and the Politics of Time”, *SSRN* (April 25, 2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2256370.

Stevens, Tim. “Cyberweapons: An Emerging Global Governance Architecture”, *Palgrave Communications*, Vol. 3 (January, 2017).

Stevens, Tim. “Cyberweapons: Power and the Governance of the Invisible” (Forthcoming).

Strauss, Anselm L. *Qualitative analysis for social scientists* (Cambridge University Press, 1987).

Tannenwald, Nina. “The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use”, *International Organization*, Vol. 53, No. 3 (Summer, 1999), 433 - 468.

Teglskov, Jeppe Jacobsen and Jens Ringsmose. “Cyber-bombing ISIS: why disclose what is better kept secret?”, *Global Affairs*, Vol. 3, No. 2 (2017), 125 - 137.

Tiezzi, Shannon. “The US and China's Common Interest: Cyber Spying”, *The Diplomat*, December 11, 2013 (accessed June 2018), https://thediplomat.com/2013/12/the-u-s-and-chinas-common-interest-cyber-spying/.

Toje, Asle. “The EU Security Strategy Revised: Europe Hedging Its Bets”, *European Foreign Affairs Review*, Vol. 15, No. 2 (May, 2010), 171 - 190.

Tumkevič, Agnija. “Cybersecurity in Central Eastern Europe: From Identifying Risks to Countering Threats”, *Baltic Journal of Political Science*, No. 5 (December, 2016), 73 - 88.

Tumkevič, Agnija. “Uncertain Security Community: Building Western Cybersecurity Order”, in *ECCWS 2017 16th European Conference on Cyber Warfare and Security*, edited by Mark Scanlon and Neihn-An Le-Khac (ACPIL, June 12, 2017), 497 - 505.

Valeriano, Brandon and Ryan C. Maness. “The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–2011”, *Journal of Peace Research*, Vol. 51, No. 3 (2014), 347 - 360.

Valeriano, Brandon and Ryan C. Maness. *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford University Press, 2015).

Vinik, Danni. “America’s secret arsenal”, *Politico*, September 12, 2015 (accessed June 2018), https://www.politico.com/agenda/story/2015/12/defense-department-cyber-offense-strategy-000331.

Weaver, Nicholas. “Is the NSA Doing More Harm Than Good in Not Disclosing Exploits?”, *Foreign Policy*, September 25, 2017 (accessed June 2018), https://foreignpolicy.com/2017/09/25/is-the-nsa-doing-more-harm-than-good-in-not-disclosing-exploits-zero-days/.

Weigley, Russel Frank. *The American Way of War: A History of United States Military Strategy and Policy* (New York: Macmillan, 1973).

Wendt, Alexander. “Anarchy is what States Make of it: The Social Construction of Power Politics”, *International Organization*, Vol. 46, No. 2 (Spring, 1992), 391 - 425.

White House. *The National Strategy to Secure Cyberspace* (Washington, DC, February 2003).

White House. *National Security Strategy 2010* (Washington DC, White House, May 2010).

White House. *International Strategy for Operating in Cyberspace. Prosperity, Security, and Openness in a Networked World* (Washington, DC, May 2011).

White House. *National Security Strategy 2015* (Washington, DC, February 2015).

White House. *National Security Strategy 2017* (Washington, DC, December 2017).

Wilding, Nick. "Cyber resilience: How important is your reputation? How effective are your people?", *Business Information Review*, Vol. 33, No. 2 (2016), 94 - 99.

Williams, Major General Brett T. "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Forces Quarterly*, No. 73, (2nd Quarter, 2014), 12 - 19.

Winterfeld, Steve and Jason Andress. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice* (Syngress, 2013).

World Economic Forum. *Advancing Cyber Resilience Principles and Tools for Boards* (January, 2017). Available at: http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf.

Zheng, Ren, Wenlian Lu, and Shouhuai Xu. "Active Cyber Defense Dynamics Exhibiting Rich Phenomena", in *Proceedings of the 2015*

Symposium and Bootcamp on the Science of Security, Article No. 2 (April, 2015).