RESEARCH PAPER
JULY 2022

PROPAGANDA AND CYBERTERRORISM IN THE CYBER DOMAIN: IS DETERRENCE STILL VALID IN CYBERSPACE?

MARIA GIULIA TRENTI

UNIVERSITÀ DEGLI STUDI FIRENZE

Center for Cyber Security and International Relations Studies

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,

Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Le dichiarazioni e le opinioni espresse nella presente relazione sono unicamente quelle dell'autore e non implicano l'approvazione da parte dell'Università di Firenze, del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali o del Center for Cyber Security and International Relations Studies.

Center for Cyber Security and International Relations Studies

PROPAGANDA AND CYBERTERRORISM IN THE CYBER DOMAIN: IS DETERRENCE STILL VALID IN CYBERSPACE?

Maria Giulia Trenti

UNIVERSITÀ DEGLI STUDI FIRENZE

Research Paper

July 2022

THEORETICAL FRAMEWORK

The technological development of recent decades has led to ever new and mind-blowing technologies and has paved the way for what has been defined by NATO in 2016 as the fifth domain, to be added to the traditional four: Cyberspace.

Cyberspace has opened up endless possibilities and at the same time enormous risks for each actor that operate in it.

International relations have moved into cyberspace, as has the management of security and state infrastructure.

This new domain, however, has also led to the birth of new players: the dynamics of traditional power are facing a potentially uncontrollable environment.

Within this new environment there are threats that were previously unthinkable and difficult to control for states, many times unprepared to deal with certain problems.

It will be very interesting to analyze the relationship between two actors who have opposites intensions in cyberspace, but constantly in contact: states and terrorists.

Among the many points of contrast, one aspect is the most challenged in this tension: Deterrence.

This paper will analyze this aspect and link it specifically to the threats that deterrence suffers from non-state actors and criminals such as cyberterrorists.

What are the advantages that cyberspace offers to terrorists?

It will be really interesting to link all that said to the very characteristics of cyberspace and understand what implications they have and how they contribute: which of the two agent is most facilitated by the characteristics of cyberspace?

We will see how state actors are the most disadvantaged by the characteristics of cyberspace in terms of deterrence.

Focusing on this aspect I ask myself the following research question: is deterrence still valid in cyberspace?

The conclusion will be an open question, still undefined and leaving open future scenarios of analysis that will be really interesting to examine in 10 years from now.

Literature review

The following work started from a specific research question: Propaganda and Cyberterrorism in the Cyber Domain: Is Deterrence still Valid in Cyberspace?

To answer this question, a critical analysis and theoretical investigation has been conducted on the validity of Deterrence in cyberspace that rests on the basis of theories and essays realized by important authors of the cyber field and not only.

First analyzing cyberspace per sè, using the definitions of Kramer (2009); Mayer, Martino, Mazurier, Tzvetkova (2014); and the United Nations (2016).

Then was analyzed the concept of information disorder, specifically in the aspects of propaganda and misinformation, using studies conducted both by Wardle and Derakhshan (2017) and by the European Parliament (2019).

These elements were linked to the concept of security and its tension and relationship with democracy, specifically using the work of Van Puyvelde and Brantly (2019).

Using the work of Weimann (2004) in the Special Report of United State Institute of Peace and the one of Giantas and Stergiou (2018) it was possible to analyze the phenomenon of cyberterrorism.

It was included in this work also a quick analysis of a real cyber terroristic attack in France in 2015 against the television network TV5Monde, in order to introduce the problems related to attribution and deterrence in cyberspace.

Starting from the definition of Shelling (1996), the theme of deterrence was addressed, both theoretically and critically, linking it to the problems and challenges that come from cyberspace.

The conclusions highlighted the need to adapt the techniques of physical deterrence to cyberspace, but with an open viewpoint in accordance with the evolving dynamics of cyberspace.

Summary

PROPAGANDA AND CYBERTERRORISM IN THE CYBER DOMAIN: IS DETERRENCE STILL VALID IN CYBERSPACE?

INTRODUCTION

Preliminarily to the discussion regarding the validity of deterrence in cyberspace, considering specifically the implications of Cyberterrorism and propaganda in the cyber domain, it is important to focus on some practical definition of the terms under consideration, and of other elements conducive to a critical analysis of this phenomena.

According to Kramer (2009)[1] "existing 28 different definitions of cyberspace". But we can attempt a definition saying that "[...] Cyberspace is a global and dynamic domain (subject to constant change) characterized by the combined use of electrons and electromagnetic spectrum, whose purpose is to create, store, modify, exchange, share and extract, use, eliminate information and disrupt physical resources" (Mayer et al., 2014)[2].

Cyberspace is both composed by a physical and virtual dimension and was defined back in 2016 by NATO as a domain[3].

To be more specific, cyberspace has itself some distinctive characteristic: the volatility, because of the fact that it change constantly;

---

[1] Kramer, F. (2009). *CHAPTER 1 Cyberpower and National Security: Policy Recommendations for a Strategic Framework*. Page 1. [online] Available at: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-01.pdf?ver=2017-06-16-115055-617 [Accessed 1 Jun. 2022].

[2] M. Mayer, L. Martino, P. Mazurier and G. Tzvetkova, (2014). *How would you define Cyberspace?*. *www.academia.edu*. Page 1. [online] Available at: https://www.academia.edu/7097256/How_would_you_define_Cyberspace [Accessed 1 Jun. 2022].

[3] In July 2016, Allies reaffirmed NATO's defensive mandate and recognized cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea.
NATO Review. (2019). NATO's role in cyberspace. [online] Available at: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

the uncertainty, related with concepts such as anonymity, identity and attribution of responsibility; the complexity, that we can define as a sort of "cyber divide" related with states' ability and infrastructure; the ambiguity, basically who detains the power.

As said before, it is necessary to provide in advance some tools for the analysis of related phenomena: such as definition of the concept of disinformation and propaganda.

According to the European Parliament Report (2019)[4] "Automated tackling of disinformation" is better to adopt the "information disorder theoretical framework"[5] to define disinformation and propaganda (Wardle and Derakhshan, 2017), that sets out three kinds of false or injurious information:

"*Mis-information: false information that is shared inadvertently, without meaning to cause harm. Dis-information: intending to cause harm, by deliberately sharing false information. Mal-information: genuine information or opinion shared to cause harm, e.g. hate speech, harassment."*

In the last two decades we have witnessed a rapid rise of online disinformation. According to the European Parliament Report (2019)[6] the reason are essentially five:

"Online propaganda and for-profit (clickbait) disinformation sites [...]; Post-truth politics, where politicians, parties and governments frame key political issues in propaganda, instead of facts [...]; partisan media [...] amplified through social media echo chambers; polarized crowds [...] characterized by flame wars and biased content sharing [...]; technological affordances of advertising algorithms and social platforms (with) technologies such as [...] personalized social feeds, and micro-targeted advertising [...]."

---

[4] www.europarl.europa.eu. (2019). Automated tackling of disinformation-Major challenges ahead | Panel for the Future of Science and Technology (STOA) | European Parliament. Page 15 [online] Available at: https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2019)624278 [Accessed 1 Jun. 2022].

[5] Wardle, C. and Derakhshan, H. (2017). *INFORMATION DISORDER : Toward an interdisciplinary framework for research and policy making*. Page 6 [online] Available at: https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

[6] Op.cit. Page 11-12

Disinformation is also related to propaganda which we can try to define using the definitions of The Institute for Propaganda Analysis (1937)[7] and Nelson (1996)[8], as "[...] a systematic form of purposeful persuasion that attempts to influence the emotions, opinions, and actions for ideological purposes" and also "[...]carried out deliberately by individuals or groups with a specific view for predetermined ends and through psychological manipulation".

All that said, what makes disinformation and propaganda so attractive and challenging to identify? The main characteristic is that those techniques are used with "the intent to deepen social division and increase polarization, and also influence public opinion, or impact key political outcomes" (European Parliament, 2019, p. 17); all this is possible because of the structure used itself: a comprehensible story with a clear distinction of good and evil, that provides sense of simple and plausible answers, all amplified also thanks to peer-to-peer distribution, and the chance of content now to go viral.

So at this point we can therefore say that cyberspace is a very powerful domain but also a tool, and as such, can be used for good or bad purposes, depending on the actors and what they make of it.

The advent of the digital world brought with it the debate on the relationship between democracy and security: initially the Internet was considered as a neutral space, which guaranteed freedom and democratization.

Then, with the development of increasingly advanced technologies, it was evident that cyberspace opened the way to new and important threats.

How and why the cyberspace is used depends on many factors: economic, political and social; in fact, according to Kuehl (2009)[9], it is

---

[7] Wikipedia Contributors (2020). *Propaganda: The Formation of Men's Attitudes*. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Propaganda:_The_Formation_of_Men%27s_Attitudes
The Institute for Propaganda Analysis 1937, inspired by Harold Lasswell. Ellul, Jacques (1965). Introduction by Konrad Kellen in Propaganda: The Formation of Men's Attitudes, pp. xi–xii. Trans. Konrad Kellen & Jean Lerner from original 1962 French edition Propagandes.

[8] Wikipedia Contributors (2019). *Propaganda*. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Propaganda
Nelson, Richard Alan (1996), A Chronology and Glossary of Propaganda in the United States pp. 232–233

[9] Op. cit.

essential "to reflect on the massive technological and social changes with which cyberspace is interwoven".

"From this perspective, cyberspace has simply provided new ground for pre-existing processes and tensions, between democracy and security, to express themselves"[10] (Van Puyvelde and Brantly, 2019)

According to Makinda's[11] definition of security as "the preservation of the norms, rules, institutions and values of society", the United Nations[12] described National security "as the ability of a state to cater for the protection and defense of its citizenry" .

The current crisis and the tensions between democracy and security also depend on the need for states to gather information to monitor and prevent any attacks and threats, such as those that come from cyberterrorism. This aspect restricts the freedom of citizens and at the same time is not able to control the crisis linked to the weaponization of information.

According to Lachow (2009)[13]:

"The term information war can be understood to refer to cyber conflict at the nation-state level involving either direct military confrontation or indirect competition via disruption and deception."

Within this complicated game of relationships and power, states also have to deal with terrorist attacks, both physical and cyber.

Cyberspace offers new frontiers, or rather, eliminates borders for non-state actors and criminals while minimizing physical risks: it offers a huge potential recruitment pool, ability to assert its power and influence with low costs but much media return and new ways of organizing and structuring criminal or terroristic organization.

---

[10] Damien Van Puyvelde and Aaron Franklin Brantly (2019). *Chapter 9.Cybersecurity and Democracy.* In *Cybersecurity : politics, governance and conflict in cyberspace*. Page 234. Cambridge, Uk ; Medford, Ma, Usa: Polity Press.

[11] National Defense University Press. (n.d.). *Cyberpower and National Security*. [online] Available at: https://ndupress.ndu.edu/Media/News/Article/1216674/cyberpower-and-national-security/

[12] ibidem

[13] Lachow, I. (2009). *CHAPTER 19 Cyber Terrorism: Menace or Myth?*. Page 4. [online] Available at: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-19.pdf?ver=2017-06-16-115055-273

The international debate places great importance on how to prevent potential threats and cyberterrorist attacks.

Although generally terrorists use cyberspace for strategic attacks, coordinated with physical attacks, to increase terror in the population and discredit state deterrence policies, the fear is that they can greatly increase their capabilities.

As we have already mentioned, cyberspace is a virtual domain with many implications, and can have important repercussions on the physical world: this is due both to its structure and to the world's increasing digitalization.

Everything is interconnected, and cyberspace is the main way to cross state boundaries in a potentially anonymous and silent way.

It's possible to re-track a clear example of the use of cyberspace to spread propaganda and terror and deepening social division in what happened on April 8th, 2015 in France, more specifically to the television network TV5Monde.

This case study also allows us to critically analyze the problems that arise related to anonymity and deterrence in cyberspace.

TENSION BETWEEN SECURITY AND DEMOCRACY: INFORMATION WAR AND THE CYBERTERRORISM THREAT.

At this point we can see that technologies, although they have implemented and greatly facilitated the organization of the daily life of citizens and states, must be considered as double-edged weapons.

New technologies and the cyberspace have opened up the possibility of accessing any part of the globe at any time, which makes it extremely difficult to regulate jurisdiction on a legal level in international relations: anyone with bad intentions can geo-reference himself anywhere avoiding jurisdictions and attributions of blame.

We are accustomed to thinking of terrorism as a violent act that causes the loss of many human lives, but cyberspace opens the door to new threats: such as coercion and intimidation.

Borrowing the question brought forth by Weimann (2004)[14] in the Special Report of United State Institute of Peace: "How real is the threat that cyberterrorism poses?".

Given what has been said so far and the increasing digitization, the risks and threat are potentially huge, depending also on what one might call the ICT "trading game": "the more technologically developed a country is, the more vulnerable it becomes to cyberattacks against its infrastructure"[15].

To answer the question: "Although cyberterrorism does not entail a direct threat of violence, its psychological impact on anxious societies can be as powerful as the effect of terrorist bombs. Moreover, the most destructive forces working against an understanding of the actual threat of cyberterrorism are a fear of the unknown and a lack of information or, worse, too much misinformation"[16].

In order to get to the heart of the analysis of the case study, it is necessary to specify that the so-called Islamic State (ISIS) from its creations has been a "pioneer" in cyber-terrorism activities.

---

[14] Weimann, G. (2004). *Gabriel Weimann Cyberterrorism How Real Is the Threat?* [online] Available at: https://www.usip.org/sites/default/files/sr119.pdf
[15] Ibidem. Page 2
[16] Ibidem. Page 3

Regarding that is important to emphasize that there are "specific lines separating the concept of cyber-terrorism from cyber-crime"[17] (Giantas and Stergiou, 2018):

"The key element that distinguishes an act of cyber terrorism from a cybercrime is that the first contains the element of terror. Cyber-terrorist attacks cause terror and a sense of insecurity by causing extensive disturbances. Furthermore, an essential feature of cyber terrorism [...] is the existence of political expediency of an extremist actor."

Case Study: TV5Monde under cyber terroristic attack? Problem of attribution

TV5 Monde, it's a global television network founded by the French government in 1984 that broadcasts news and other programs produced in France, Belgium, Switzerland and Canada.

On 8 April 2015, TV5 Monde inaugurated its new thematic channel on the "French art de vivre", in the presence of Foreign Minister Laurent Fabius; and was attacked by the Cyber Caliphate, "one of the first cyber-terrorist groups to support the Islamic State" (Giantas and Stergiou, 2018)[18].

The Hackers simultaneously blacking out 11 channels and taking over the network's website and social media accounts of the television network, spreading propaganda content also with some reference at the terrorist attack to Charlie Hebdo newspaper early the same year.

Authorities confirm that the attack "could not have been carried out by a single individual but by a group of several dozen high-profile pirates, who could have been hired as mercenaries"[19].

---

[17] Giantas, D. and Stergiou, D. (2018). From Terrorism to Cyber-Terrorism: The Case of ISIS. *SSRN Electronic Journal*. Page 4-5 [online] Available at: https://www.academia.edu/36097787/From_Terrorism_to_Cyber_terrorism_The_Case_of_ISIS [Accessed 1 Jun. 2022].

[18] Ibidem. Page 10

[19] it.frwiki.wiki. (n.d.). *Attacco informatico contro TV5 Monde - frwiki.wiki*. [online] Available at: https://it.frwiki.wiki/wiki/Cyberattaque_contre_TV5_Monde [Accessed 1 Jun. 2022].

For The France National Information Systems Security Agency (NISSA) "engineers the attack was prepared long ago and meticulously"[20].

The investigation indicates that hackers used the technique of phishing by sending an email in late January to all journalists of the channel: responding to those email allowed the hackers to access the chain's network and circulate whenever they wanted via a Trojan horse.

After several months since the attack, media revealed that the investigation has moved away from the jihadist trail, seen as a bait, and turned towards a group of Russian hackers called APT28 because of the similarities to the modus operandi of this group:

"[...]use common servers, and the source code has been typed on a Cyrillic keyboard sometimes corresponding to office hours in Saint Petersburg and Moscow"[21].

According to the investigation, this change of trail is plausible because the attack has happened in a context of deterioration of the relations between France and Russia "as a result of the suspension of the delivery of two Mistral ships on the background of the (2015) Ukrainian crisis"[22].

This attack had costed a lot to the French network, obviously to be considered as an incomparable damage compared to the loss of lives recorded after physical terrorist attacks both previous and subsequent to this one.

Certainly, however, in addition to the physical implications of the virtual domain of cyberspace, this quickly analyzed event, also because not over in terms of investigation, raises interesting questions and also worrying ones in terms of deterrence and attribution of responsibility in cyberspace.

According to Giantas and Stergiou (2018) we can analyze the dangerous advantages that cyberspace offer to terrorist, in comparison of "physical" terrorism:

"cyber-terrorism absorbs fewer resources than the conventional terrorism, in term of methods and financial resources [...] and ensures anonymity and protection of identity [...]. As a result, the detection and identification of the extremists by the security agencies become difficult and technologically

[20] ibidem
[21] ibidem
[22] ibidem

complex. Cyber-space (also) offers a great variety and number of potential targets [...] because actors which are active in cyberspace include state governments, businesses, individuals and various organizations. Lastly, cyber-terrorism is not limited by geographical boundaries [...] and can therefore be carried out remotely from anywhere in the world"[23].

Is deterrence still valid in cyberspace, specifically considering the implication of cyberterrorism?

According to Shelling (1996) definition, "deterrence means dissuading someone from doing something by making them believe that the cost to them will exceed their expected benefit."[24]

In international law, the classic deterrence theory provide two main mechanisms: a credible threat of punishment for an action (deterrence of punishment); and denial of gains from an action (deterrence of denial).

As we know, the cyber domain is characterized by anonymity and diffusion of power: so there is no state owned-monopoly, and the usual traslatio imperi is no more possible in cyberspace, in which all depends on tools and if those tools can influence policy making.

The level of uncertainty and anonymity is so high in cyberspace that there is no assurance of the destruction of the attacking, and no way to estimate how much cost would need to be paid by the attacker in terms of retaliation.

In international relations, the tendency is to downplay both Deterrence by Denial and Deterrence by Punishment:

- In the first case, there is a cost-benefits calculus that is fundamental for the state to survive, indeed for non-state actors or terrorist it's not a limitation in action;
- In the second case, because of the attribution problem. Some factors that influence and limit the possibility of punishment are: the uncontrolled and unpredictable

[23] Op.cit. Page 6-7
[24] Shelling, T. (1996). *To prevent from action by fear or consequences*.

evolution of cyberspace and anonymity, that implies also problems in distinguishing enemy or ally.

Considering these aspects, it is necessary to add that deterrence has as main requirement the specificity, which is essential in order to estimate the exact punishment.

According to Van Puyvalde and Brantly (2019):

"Specificity at the state level is the identification of which acts perpetrated by another state constitute a violation that would cross a pre-identified "red line" or core interest of a state. Specificity within states is codified as acts that violate law. A violation by a state or non-state actor can both cross a "red line" and violate the national laws of the state it is attacking"[25].

With regard to the concept of deterrence, both in the cyber and in the physical world, it is essential to remember the need to respond quickly: an element that greatly affects the credibility of a state.

Obviously, the dynamics listed so far clarifies the difficulty that states encounter in cyberspace, in which the timing is not dictated only by the states' capacity in terms of tools and infrastructure, but also the ability of hackers to hide their tracks in an environment that has made anonymity a central feature.

[25] Damien Van Puyvelde and Aaron Franklin Brantly (2019). *Chapter 8. Organizing Deterrence and Defense in Cyberspace.* In *Cybersecurity : politics, governance and conflict in cyberspace*. Page 221. Cambridge, Uk ; Medford, Ma, Usa: Polity Press.

CONCLUSIONS

To conclude, we can summarize saying that cyberspace presents some important challenges for states in the field of deterrence.

These challenges can be classified into two interrelated categories: the structural challenges, due precisely to the very structure of cyberspace: in continuous evolution, complex and vulnerable; and the challenges related to Deterrence in the strict sense, such as the proportionality of penalty, and the problems of attribution.

The first challenge is certainly anonymity, which brings with it great problems of attribution.

This aspect is also linked to the problem of the countermove: because the response must be rapid in order not to undermine the credibility of a state.

We can add that speed in cyberspace is not an easy element to manage: although it is a very important feature of this constantly evolving domain, it is an enemy of deterrence, which requires accuracy and specificity: a counter-move too fast could be inaccurate, but at the same time long waits are to be avoided because they expose to new and constant vulnerabilities.

Another element to be taken into account is the proportionality of penalty.

The extent of the punishment is unclear to determine, in fact cyberspace is a relatively new domain, in constant evolution.

Continuous evolution brings with it another challenge: predictability.

It is not a given, that the states are able to anticipate an attack in advance, and especially its extent.

The possibilities that cyberspace opens up are multiple and potentially infinite, and so, while one state develops certain infrastructures, one criminal entity can develop others, and even more effective ones.

The logic of cost-benefit greatly affects the freedom of state action, but touches very little malicious actors, which, as we have seen, draw many advantages from using cyberspace.

Returning to the initial question: Is deterrence still valid in Cyberspace? It is clear from this analysis that this remains an open question.

The future of cyberspace is uncertain, we know that it is a constantly expanding domain and increasingly present in the state infrastructure and beyond.

Surely it emerges clearly the need to structure new deterrence techniques in continuity with the existing ones but more easily adaptable to the needs of cyberspace.

REFERENCES

- Brunst, P. W., (2013). CHAPTER 2. Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet. In Wade, M. and Almir Maljević (2013). A war on terror? the European stance on a new threat, changing laws and human rights implications. New York ; Heidelberg ; Dordrecht ; London Springer. [online]. Available at:

https://sites.les.univr.it/cybercrime/wp-content/uploads/2017/08/brunst.pdf [Accessed 1 Jun. 2022].

- Dedan Kimathi University of Technology. (2017). Chapter II Cyber Crime and its Classification. [online]

Available at: https://www.bbau.ac.in/dept/Law/TM/1.pdf [Accessed 1 Jun. 2022].

https://www.coursehero.com/file/102359426/doc2pdf/ [Accessed 1 Jun. 2022].

- Damien Van Puyvelde and Aaron Franklin Brantly (2019). Cybersecurity : politics, governance and conflict in cyberspace. Cambridge, UK ; Medford, Ma, USA: Polity Press.

- Giantas, D. and Stergiou, D. (2018). From Terrorism to Cyber-Terrorism: The Case of ISIS. SSRN Electronic Journal. [online] Available at: https://www.academia.edu/36097787/From_Terrorism_to_Cyber_terrorism_The_Case_of_ISIS [Accessed 1 Jun. 2022].

- International Center for Journalists. (2018). A Short Guide to the History of 'Fake News' and Disinformation: A New ICFJ Learning Module. [online] Available at: https://www.icfj.org/news/short-guide-history-fake-news-and-disinformation-new-icfj-learning-module [Accessed 1 Jun. 2022].

- idsa.in. (n.d.). Suchak Patel asked: What is the meaning of 'Deterrence by Denial' especially in the context of India and China? | Manohar Parrikar Institute for Defence Studies and Analyses. [online] Available at: https://idsa.in/askanexpert/meaning-of-deterrence-by-denial-especially-the-context-india-china#:~:text=In%20Deterrence%20by%20Denial%2C%20the [Accessed 1 Jun. 2022].

- it.frwiki.wiki. (n.d.). Attacco informatico contro TV5 Monde - frwiki.wiki. [online] Available at: https://it.frwiki.wiki/wiki/Cyberattaque_contre_TV5_Monde [Accessed 1 Jun. 2022].

- Kramer, F. (2009). CHAPTER 1 Cyberpower and National Security: Policy Recommendations for a Strategic Framework. [online] Available at: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-01.pdf?ver=2017-06-16-115055-617 [Accessed 1 Jun. 2022].

- Kuehl, D. (2009). CHAPTER 2 From Cyberspace to Cyberpower: Defining the Problem. [online] Available at: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210 [Accessed 1 Jun. 2022].

- Kwast, S. and Hayden, D. (n.d.). Air University. [online] Available at: https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF [Accessed 1 Jun. 2022].

- Lachow, I. (n.d.). CHAPTER 19 Cyber Terrorism: Menace or Myth?. [online] Available at:

https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-19.pdf?ver=2017-06-16-115055-273 [Accessed 1 Jun. 2022].

- Mayer, M., Martino, L., Mazurier P. Tzvetkova G., (2014*). How would you define Cyberspace?*. Experimental online laboratory, PhD in Politics, Human Rights and Sustainability, Scuola Superiore Sant'Anna. www.academia.edu. [online] Available at:

https://www.academia.edu/7097256/How_would_you_define_Cyberspace [Accessed 1 Jun. 2022].

- National Defense University Press. (n.d.). Cyberpower and National Security. [online] Available at: https://ndupress.ndu.edu/Media/News/Article/1216674/cyberpower-and-national-security/ [Accessed 1 Jun. 2022].

- NATO Review. (2019). NATO's role in cyberspace. [online] Available at: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html [Accessed 1 Jun. 2022].

- Oakton, M. (2016). Autopsy of Cyber Attack on TV5Monde. [online] Infosec Partners. Available at: https://www.infosecpartners.com/autopsy-of-cyber-attack-on-tv5monde [Accessed 1 Jun. 2022].

- Osisanya, S. (n.d.). National Security versus Global Security. [online] United Nations. Available at: https://www.un.org/en/chronicle/article/national-security-versus-global-security [Accessed 1 Jun. 2022].

- Trujillo, C. (2014). The Limits of Cyberspace Deterrence. [online] p.43. Available at:

https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-75/jfq-75_43-52_Trujillo.pdf [Accessed 1 Jun. 2022].

- Wardle, C. and Derakhshan, H. (2017). INFORMATION DISORDER : Toward an interdisciplinary framework for research and policy making. [online] Available at: https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c [Accessed 1 Jun. 2022].

- Weimann, G. (2004). Gabriel Weimann Cyberterrorism How Real Is the Threat? [online] Available at: https://www.usip.org/sites/default/files/sr119.pdf [Accessed 1 Jun. 2022].

- Wikipedia Contributors (2020). Propaganda: The Formation of Men's Attitudes. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Propaganda:_The_Formation_of_Men%27s_Attitudes [Accessed 1 Jun. 2022].

- Wikipedia Contributors (2019). Propaganda. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Propaganda [Accessed 1 Jun. 2022].

- www.europarl.europa.eu. (2019). Automated tackling of disinformation-Major challenges ahead | Panel for the Future of Science and Technology (STOA) | European Parliament. [online] Available at:

https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2019)624278 [Accessed 1 Jun. 2022].

- www.cbsnews.com. (n.d.). ISIS-allied hackers claim worrying new attack. [online] Available at: https://www.cbsnews.com/news/french-tv-network-tv5-monde-

hacked-by-cybercaliphate-in-name-of-isis/ [Accessed 1 Jun. 2022].

.

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Center for Cyber Security and
International Relations Studies