Influence operations in cyberspace

On the applicability of public international law during influence operations in a situation below the threshold of the use of force

Pijpers, B.M.J.

Publication date
2022

Chapter 2

CHAPTER 2: INFLUENCE OPERATIONS – THE CONCEPT

In the previous chapter the baselines on influence, cyberspace and its attributes were outlined, and it was deduced that influence operations inherently fall below the threshold of the (threat or) use of force.

This present chapter describes the characteristics of influence operations in cyberspace. The first section contains a concept for influence operations.

The second section outlines the operationalisation of the concept, thereby addressing the instruments of power a State can use to influence other States to protect or promote its national interests; how it uses cyberspace to engage in, and influence, the targeted audiences of the political systems of other States. Furthermore, this section explores why the audiences are susceptible to influence operations; how the influence operation affects the political system and whether it changes the behaviour or the attitude of the targeted State. The operationalisation of influence operations will be augmented with examples of generic Russian influence operations, illustrating how influence operations are executed and what effects they bring about.[1]

Finally, an answer will be given to the sub-question: *"What are the characteristics of influence operations, what mechanisms of influence can be applied and how does cyberspace affect influence operations?*

The chapter produces an operational framework for influence operations in cyberspace that can be applied to analyse the three cases of influencing operations as will be described in Chapter 4. Together with the legal framework depicted in the next chapter, these frameworks will serve to analyse the influence operations in Chapter 5 and 6.

1 The reason to choose the influence operations with the Russian Federation in a lead role is because these appear most successful. See: Jean Baptiste Jeangene Vilmer, "Information Manipulation: A Challenge for Our Democracies," *CAPS of the Ministry for Europe and Foreign Affairs and IRSEM of the Ministry for the Armed Forces*, 2018. pp. 49-50; see also: Andreï Soldatov and Irina Borogan, The Red Web : The Kremlin's Wars on the Internet, First Edit (New York: PublicAffairs, 2017).; Keir Giles, "Handbook of Russian Information Warfare," *NATO Defence College* 9, no. November (2016): 1–90. pp. 16-30. For an overview of RF influence operations see: Booz Allen Hamilton, "Bearing Witness: Uncovering the Logic behind Russian Military Cyber Operations," *Booz Allen Hamilton*, 2020. pp. 11-36; Nicu Popescu and Stanislav Secrieru, "Hacks, Leaks and Disruptions," 2018. pp. 19-20.

Section 2.1.: The conceptual framework

"My intuitive idea of power then, is something like this: A has power over B to the extent that he can get B to do something that B would not otherwise do"[2]

The conceptual framework offers a generic design of how a State or political system (A) influences another actor (B) in cyberspace without the use of force.[3] The conceptual framework will provide a systemic breakdown of influence operations starting from the intent of the political system of State A, deriving from the need to protect or further national interests. After a decision has been taken to act, an array of instruments of power will be mobilised to accomplish the intent as laid down in a strategy. Executing and exploiting influence operations in cyberspace results in an engagement of State A with the targeted audiences of the political system of State B via cyberspace. The consequence of the engagement can be a change in the behaviour of State B directly, or indirectly via a change in the attitude of the political system of State B, affecting the ideology, concept or actors of the State. A full overview of the operationalised influence operation is given below.[4]

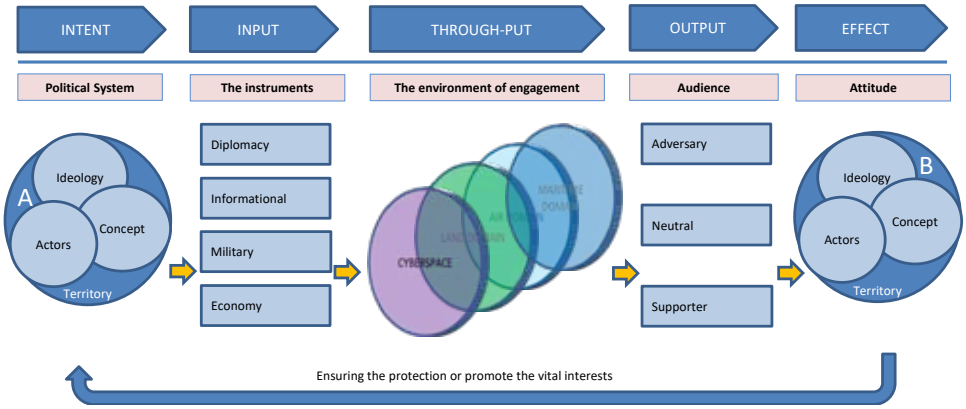

Figure 2 - 1 The concept of an operations by A to influence B

2 Robert A. Dahl, "The Concept of Power," *Behavioral Science* 2, no. 3 (1957): 201–15. pp. 202- 203.

3 The design is based on Lasswell's act of communication, Harold D. Lasswell, "The Structure and Function of Communication in Society," in *The Communication of Ideas*, ed. Lyman Bryson (New York: Harper and Row, 1948), 37–51. See also: David Easton, *The Political System: An Inquiry into the State of Political Science*, 1953.; David Easton, "An Approach to the Analysis of Political Systems," *World Politics* 1, no. Vol 9, No 3 (1957): 383–400. Paul A.L. Ducheine and Jelle Van Haaster, "Fighting Power, Targeting and Cyber Operations," *International Conference on Cyber Conflict, CYCON*, 2014, 303–27.

4 Note that this model is not meant to represent reality, but merely to give a conceptual reflection of influence operations. A could represent any State or coalition of States.

Section 2.2.: The operationalisation of influence operations in cyberspace

"A man may die, nations may rise and fall, but an idea lives on. Ideas have endurance without death"[5]

"The US and UK understanding of 'cyber' is predominantly technical and computer-network based, while Russia and China use a cognitive approach based on understanding of mass psychology and of how to exploit individuals"[6]

"Making decisions is like speaking prose— people do it all the time, knowingly or unknowingly"[7]

2.2.1. The Political System

Easton and Almond were among the first to create a functional empirical system for politics, entailing an input, output and feedback functionality.[8] According to Easton, political systems comprise political actions, political roles and groups, and the 'boundary of the political system is defined by all those actions more or less directly related to the making of binding decisions for a society'.[9]

The political system allocates values by means of polities, and these allocations are authoritative and binding for the society as a whole.[10] Almond and Coleman elaborate on Easton's concept, stating that a political system is a 'legitimate, order-maintaining or transformational system in the society',[11] meaning that a political system not only allocates values, but includes political and societal interactions, such as elections.[12]

5 J.F. Kennedy, in Jo Brick, "The #Future of War and the Fight for the Strategic Narrative," *Strategic Bridge* 2015 (2015). p. 1.

6 Public Administration and Constitutional Affairs Committee House of Commons, "Lessons Learned from the EU Referendum," 2017.

7 Daniel Kahneman and Amos Tversky, "Choices, Values, and Frames," *American Psychologist* 39, no. 4 (1984): 341–50. p. 341.

8 J.G. Gunnell, "The Reconstitution of Political Theory: David Easton, Behavioralism, and the Long Road to System," *Journal of the History of Behavioral Sciences* 49, no. 2 (2013): 190–210., p. 193.

9 Easton, "An Approach to the Analysis of Political Systems." p. 385.

10 Easton, *The Political System: An Inquiry into the State of Political Science*. p.13.; Steven J Barela, "Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion," *Just Security*, 2017.

11 Gabriel A Almond and James S Coleman, The Politics of the Developing Areas, Princeton University, Center of (Princeton, N.J. SE - xii, 591 p. : illustrations ; 24 cm: Princeton University Press, 1960). p. 7.

12 In political science a State would be defined as the totality of permanent power structures representing and governing people in a territory, see: Booz Allen Hamiltion, "Bearing Witness: Uncovering the Logic behind Russian Military Cyber Operations." p. 1. (note b).

Political systems encapsulate the political power of a society and are therefore both the main 'target' when addressing State B, as well as the source of power of State A – the author State. The power State A holds is employed to persuade, manipulate, deter or compel other actors in order to generate political change. Power, in this sense, can be described as 'the ability of one State to marshal its resources in order to promote its interests against the interests of another."[13] Or in other words: power is the capability to persuade or dissuade other actors,[14] whether they are a friendly or an antagonistic audience.[15] Power is a relational capability and is context-dependent.[16]

A political system has three closely interrelated elements which constitute the foundation of its power,[17] namely the ideology of the political system, the concept and the actors. [18] The political system is set in a territorial context, embodied in a State's characteristics such as geography, infrastructure, natural riches, the size of its territory which all contribute to the rudimentary physical power of a State.[19]

The ideology of the political system entails the worldview, mind-set and perception of a State, which may stem from schools of thought with a communist or liberalist signature but can also have less paternalistic origins in case of an authoritarian rule.

The conceptual element describes how the political system operates and involves the roles or functions of a political system,[20] which include national defence, elections, law enforcement, diplomacy and taxation. There is a close link with the ideology of the political system - a liberal democracy differs in structure and organisation from a society based on anarchic, authoritarian or communist ideology.

13 David J. Betz and Tim Stevens, "Power and Cyberspace," *Adelphi Series* 51, no. 424 (2011): 35–54. p. 43.

14 Morgenthau defines power as 'anything that establishes and maintains the control of man over man'. See: Hans J Morgenthau, *Politics among Nations : The Struggle for Power and Peace* (New York: New York, 1950). pp. 4-15.

15 William Hutchinson, "Influence Operations: Action and Attitude," *Proceedings of the 11th Australian Information Warfare and Security Conference*, no. December (2010). p. 16.

16 Joseph S. Nye Jr., "Soft Power," *Foreign Policy*, no. 80 (1990): 153–71. p. 160; Simon. Reich and Richard Ned. Lebow, *Good-Bye Hegemony!: Power and Influence in the Global System* (Princeton, New Jersey: Princeton University Press, 2014). p. 5; Joseph S. Nye Jr., "Cyber Power," 2010. p. 3.; Dahl, "The Concept of Power." pp. 205-209.

17 Dahl, "The Concept of Power." p. 203: "the base of an actor's power consists of all the resources – opportunities, acts, objects, etc – that he can exploit in order to effect the behaviour of another'.

18 Dahl describes the political system Dahl describes the political system as an ecosystem of procedures, processes and actors: the institutions (parliament, cabinet, government, ministries); the electoral system; the political parties; the leaders (president, PM, traditional, charismatic, legality); the type (representative democracy, aristocracy); the media (journalists); legitimacy and legality. Robert A. Dahl, Modern Political Analysis (Englewood Cliffs, NJ: Englewood Cliffs, NJ : Prentice-Hall, 1963). pp. 76-82.

19 Betz and Stevens, "Power and Cyberspace." p. 43.

20 In Almond and Coleman, The Politics of the Developing Areas. pp. 17 and 26-57. Four 'input' functions - political socialisation and recruitment, interest articulation, interest aggregation, political communication- and three 'output' functions - rule-making, rule-application, rule adjudication - are recognised.

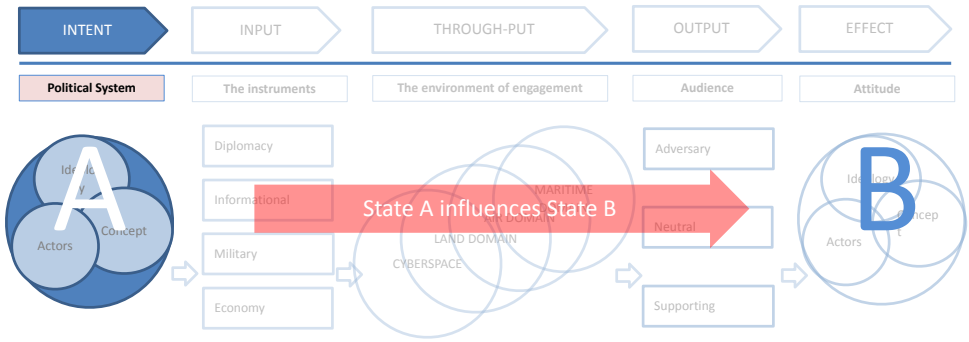

Figure 2 - 2 Influence political systems

The actors are the persons and institutions performing the roles and functions within a political system, which includes parliament and the armed forces. Political parties, parliamentary journalists and trade unions are also actors in the political system since they embody the checks and balances of that system.

The elements (ideology, concept and actors) of the political system embody the attitude to the system. These elements, which include the legal system or governmental constellation, are the sole prerogative of the political system, free from interference from other States.[21] Though the political system is passive in nature, it is not inactive. The political system engages in activities to sustain that system. This behaviour that derives from the elements of power of the political system, such as popular representation, governmental decision-making, elections or ruling a verdict, has an inherently internal character, hence is not meant for interacting with, or influencing external parties.

Before engaging in influence operations, State A will need to define an objective or intent. The intent of the State is part of, or derives from, its attitude and perception of the world and will serve to further and protect the shared values or interests of that society or State. The vital interests of a State are both the result of the 'power base'[22] of a political system and its guide: they are interdependent. There is no universal set of vital interests; the strategic culture, religion, geography or history of a State contribute to the differences in and appreciations of vital interests.[23]

21 Unless the interference is based on obligations stemming from international law or the interference is consented upon. See also Chapter 3.

22 Dahl, "The Concept of Power." p. 205.

23 For instance: the Netherlands vital interests are territorial security, economic security, ecological security, physical security, political and social stability, and protection of the international legal order. Netherlands National Coordinator Terrorism & Security, "National Security Strategy," 2019. p. 4.

To illustrate, the current Russian Federation's (RF) intent when executing influence operations could best be described as creating strategic confusion[24] in Western democratic States. Influence operations, spreading alternative narratives and truths will erode the trust in liberal freedoms and generate the sense that nothing can be trusted.[25] The RF intends to induce a long-term confrontation of beliefs, understanding and emotions so opponents are unable to assess what is true and what is not. Russia seeks to undermine liberal democracies by means of alluding to the success and strength of the autocratic form of government of the RF and the concept of Russkiy Mir (Russian World).[26] Furthermore it aspires to sow distrust in Western institutions and destabilise societies with the goal to undermine, or ensure the failure of transatlantic pro-Western government and leadership and to weaken NATO and the EU.[27]

To activate the attitude of a State, instruments of power must be mobilised. Opposing vital interests between political systems can be assessed as merely passive differences of opinion, perception or geopolitical outlook. States can choose to accept and tolerate the differences but can also decide on a more affirmative stance. If State A persists and wants to persuade or compel State B to adhere to its views and system, it will need to activate or mobilise its instruments of power to engage in a contest of wills and ideology.[28] The instruments of power, as will be described in the next section, are active in nature and are utilised to engage with other political systems.

In sum, influence operations aim to target the cognitive dimension in order to alter the attitude and the behaviour of the political system of State B. To change the attitude of a State influence operations will target its political system which is the embodiment of the attitude of a society. The political system can be described as the complex of three interrelated elements: the ideology (the principles and norms); the conceptual element depicting how a political system is structured and organised, which includes the electoral system; and the actors performing the roles and functions within a political system. The political system

24 Marie Baezner and Patrice Robin, "Cyber and Information Warfare in Elections in Europe," 2017. p. 9; William Aceves, "Virtual Hatred: How Russia Tried to Start a Race War in the United States," *Michigan Journal of Race and Law* 24, no. 2 (2019). p. 193; And related to that, plausible deniability, or maintain an air of plausibility, see: Martin Kragh and Sebastian Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case," *Journal of Strategic Studies* 40, no. 6 (2017): 773–816. pp. 778 & 789; see also: William J. Broad, "Putin's Long War Against American Science," *The New York Times*, (2020).; Jeangene Vilmer, "Information Manipulation: A Challenge for Our Democracies." p. 75; Lawrence Freedman, *The Future of War: A History*, Penguin, 2017. pp. 225-227; Scott Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict* (Washington, D.C.: Georgetown University Press, 2020). pp. 13-15.

25 Michael Chertoff, "Fake News and the First Amendment," *Harward Law Review Blog*, 2017.; Peter Pomerantsev, "To Unreality — and Beyond," *Journal of Design and Science*, no. 6 (2019). pp. 11-13.

26 Alina Polyakova et al., "The Kremlin's Trojan Horses," 2016. p. 4; Han A.J.H. Bouwmeester, *Krym Nash: An Analysis of Modern Russian Deception Warfare*, 2020. pp. 333-335.

27 Andrew Radin, Alyssa Demus, and Krystyna Marcinek, "Understanding Russian Subversion: Patterns, Threats, and Responses," no. February (2020). pp. 4-5.

28 Or as Gartzke states: "States and nonstate actors make war to further their interests when incompatibilities exist between those interests, and when alternative methods of conflict resolution are deemed ineffective or inefficient." Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back down to Earth," *International Security* 38, no. 2 (2013): 41–73, p. 54.

holds the power of a society with the purpose of 'authoritative allocation of values',[29] and intends to further and protect the shared values or (national) interests of that State.

2.2.2. Instruments of power

The instruments of power of State A are the tools that are activated once an attitude is transformed into behaviour. These instruments are meant for the engagement with State B, hence they have an external purpose, are active in nature, and represent the mobilised elements of the political system. The instruments of power of State A can be used to target the elements of the political system of State B with the intent to influence the attitude and consequently change the behaviour of State B.

To implement influence operations a range of instruments is available to the State, such as diplomacy, information, military means, economy, culture and knowledge (DIME-CK).[30] These are archetypal instruments of power and not meant to be an exhaustive, all-inclusive overview of State powers.[31] The instruments of power used by State A are deliberate activities with a clear purpose and intent. State A can use and assign the combination of instruments of power[32] to plan and execute a strategy[33] to 'unleash the power'[34] of the political system.

29 Easton, *The Political System: An Inquiry into the State of Political Science*. p. 130.

30 The instruments of power were already mentioned in Myres S. McDougal and Florentino P. Feliciano, "International Coercion and World Public Order: The General Principles of the Law of War," *The Yale Law Journal* 67, no. 5 (1958): 771–845. p. 792., McDougal et al. refer to the 'ideological' instrument instead of the informational. But see also Nye Jr., "Soft Power." p. 155; Paul A.L. Ducheine and Peter B.M.J. Pijpers, "The Missing Component in Deterrence Theory: The Legal Framework," in *Deterrence in the 21st Century—Insights from Theory and Practice*, ed. Frans P.B. Osinga and Tim Sweijs (Springer, 2021), 475–500. Pp 481-482; The definition RAND provides is: "Influence operations are the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post conflict to foster attitudes, behaviors, or decisions by foreign target audiences that further (…) interests and objectives". See: Eric V. Larson et al., *Foundations of Effective Influence Operations*, 2009. p 2.

31 Other instruments of power are legal, intelligence and finance. See: Sam Arwood, *Cyberspace as a Theater of Conflict : Federal Law, National Strategy and the Departments of Defense and Homeland Security* (Biblioscholar, 2007). pp. 67-69. Ducheine and Pijpers, "The Missing Component in Deterrence Theory: The Legal Framework." pp. 485-487; Rodgrigo Vazquez Benitez, "Legal Operations: The Use of Law as an Instrument of Power in the Context of Hybrid Threats and Strategic Competition," *NATO Legal Gazette*, no. 41 (2020): 138–44. Pp 140-141; Lin introduces law enforcement as an instrument, Herbert Lin, "Responding to Sub-Threshold Cyber Intrusions," *Georgetown Journal of International Affairs* 12 (2011). p. 132. But, also the 'surveillance' – the collection and procession of personal data - can be seen as an instrument of power. See: Colin J. Bennett, "Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications," *Surveillance and Society* 13, no. 3–4 (2015): 370–84. p. 370. Or 'infrastructure' as alluded by Hillman; Jonathan E Hillman, "Influence and Infrastructure," 2019. DIME will be used since no acronym captures all possible instruments.

32 E.g. conditional military aid; public diplomacy, military intelligence or diplomatic threats, see also: Kragh and Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case." pp. 777-778; Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses*, 2018. pp. 6-9.

33 Betz after Freedman: "Strategy is therefore the creation and manipulation of social relations that allows for the exercise of national resources towards a common goal", or strategy is the art of unlocking the power inherent in national capacities to effect outcomes in the national interest in contest with other strategists acting in their own national interests. See, Betz and Stevens, "Power and Cyberspace." p. 43.

34 As Lawrence Freedman writes, 'it takes strategy to unleash the power inherent in this [military] capacity and to direct it towards specific purposes. Strategy is thus the creative element in any exercise of power.' See: Lawrence Freedman and Srinath Raghavan, "Coercion," in *Security Studies: An Introduction*, ed. Paul D. Williams, 2008, 216–28. p. 217.

Diplomacy is the main instrument for engaging with foreign audiences in advancing or articulating the values, interest and objectives of the political systems, hence the 'characteristic channels and rituals of inter-elite or inter-official communications and negotiations'.[35] Diplomacy is mainly a persuasive tool to influence,[36] but could have a compelling or deterring impact. Diplomatic measures with an external exposure are *inter alia* (i.a.) summoning ambassadors, public diplomacy,[37] rhetoric and persuasive speeches,[38] opening embassies, signing or terminating treaties, enhancing good offices, issuing visa, releasing communiques, organising international force, as well as ending relations with another State, extradition, expulsion, sanctions or declaring a foreign national *persona non grata*.

Using the economy as an instrument can mean maintaining control of access to the flow of goods, services, money and markets, while denying access to target States.[39] Economic leverage can be used in a persuasive, manipulative or compelling way to deny access to the targeted audience,[40] while maintaining one's own access, thereby retaining strategic autonomy either within a coalition or separately.[41] Economic measures with an external dimension are: trade embargos; tariffs and quotas, domestic regulations excluding foreign actors, denying access to ports, economic sanctions or incentives, foreign economic aid, finance, designing and building infrastructure abroad,[42] development aid, monetary policies, fees on foreign exchanges, and credit provisions.

35 McDougal and Feliciano, "International Coercion and World Public Order: The General Principles of the Law of War." p. 792.

36 Dale Stephens, "Influence Operations & International Law," *Journal of Information Warfare* 19, no. 4 (2020): 1–16. p. 15; Australian Government, "Opportunity Security Strength," *Foreign Policy White Paper*, 2017. p. 76.

37 Ilya Yablokov, "Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of Russia Today (RT)," *Politics* 35, no. 3–4 (2015): 301–15. p. 303.

38 Hannah Arendt, "Philosophy and Politics," *Social Research* 71, no. 3 (2004): 427–54. p. 432.

39 McDougal and Feliciano, "International Coercion and World Public Order: The General Principles of the Law of War." p. 794.

40 Gabriel Collins, "Russia's Use of the 'Energy Weapon' in Europe," *Baker Institute for Public Policy*, no. June (2017): 1–7. p. 3-4.

41 The 1948 European Recovery Program (the Marshall Plan and Morgenthau Plan) is an example of the economic instrument of power. Its goals was to rebuild war-torn regions, remove trade barriers, modernize industry, improve European prosperity, and prevent the spread of Communism. See also Lori F. Damrosch, "Politics Across Borders: Nonintervention and Nonforcible Influence over Domestic Affairs," *The American Journal of International Law* 83, no. 1 (1989): 1–50. p. 28.

42 Hillman, "Influence and Infrastructure." pp. 4, 11, 23. Hillman argues that designing and building infrastructure abroad can advance the strategic interests of States by setting standard, transfer technology and collect intelligence. Using infrastructure as an instrument directly impacts traditional foreign policy instruments including diplomacy, intelligence and military operations.

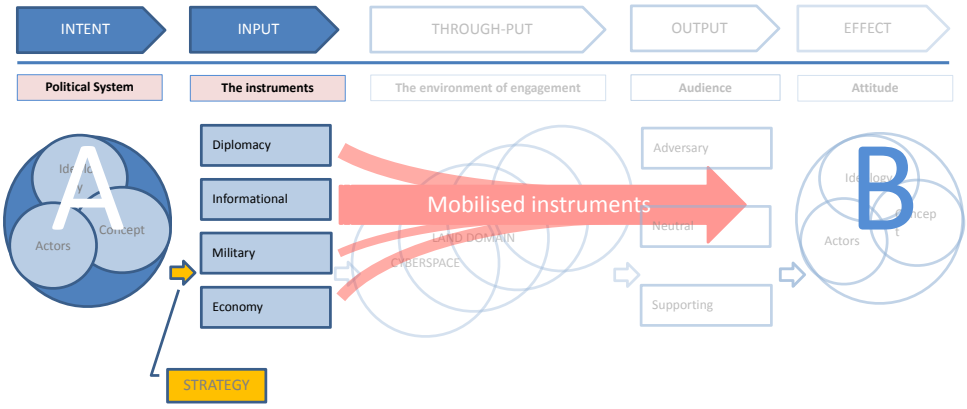

Figure 2 - 3 State A activates the instruments of power

The military instrument has long been the embodiment of the threat or the use of force in kinetic operations – the hard-power of the State.[43] It can be used for offensive or defensive kinetic deployment of power, but also for deterrence by the show of force or showing a clear sign of resolve.[44] The military instrument of power is often applied by the Armed Forces, but it is not their exclusive prerogative.[45] Military measures can also be employed for non-conflict hostile or peace-time environments, for instance via stability operations, peacekeeping operations, deterrence, or special operations.

Nye argued that, after the end of the Cold War, intangible instruments of power would come to the fore, including information, culture but also scientific power.[46] Culture is a soft power resource and relates to people's identities. It strengthens social cohesion, encompassing the way of living,[47] religion and science, tradition and innovation, art and music, language and literature.[48] Examples of institutions that use of culture as an instrument are the German Goethe Institute and the *Alliance française* which promote German and French, respectively, abroad. In contrast, there are ample examples of the banning of specific forms of cultural

43 McDougal and Feliciano, "International Coercion and World Public Order: The General Principles of the Law of War." p. 795. "While substantial degrees of coercion may be achieved by the skilled utilization of the diplomatic, ideological and economic instrument, the attainment of the maximum intensity of coercion normally requires the supplementation of such instruments with military force."; see also: Nye Jr., "Soft Power." pp. 166-167.

44 Erik Gartzke and Jon R. Lindsay, "Thermonuclear Cyberwar," *Journal of Cybersecurity* 3, no. 1 (2017): 37–48. p. 41.

45 Eric Schmitt and Matthew Rosenberg, "C.I.A. Want Authority to Conduct Drone Strikes in Afghanistan for the First Time," *The New York Times*, September 15, 2017.

46 Nye Jr., "Soft Power." p. 155.

47 Toby Miller, "Culture with Power: The Present Moment in Cultural Policy Studies," *Asian Journal of Social Science* 22, no. 1 (1994): 264–82. p. 264.

48 Ronald Grätz, "Culture as an Instrument of Social Transformation," *EU-LAC Foundation*, 2017.

expression incompliant with the existing governmental policies,[49] or the suppression of the way of living or language of many indigenous peoples.[50]

Information as an element of national power refers to the way a political system uses data and knowledge to understand and shape the complex nature of the information environment in support of national interests.[51] Cohen and Bar'el argue that the informational instrument aims to disrupt 'the opponent's ability to direct objective content to its target audience, to properly grasp reality and to establish effective defensive action capability'.[52] Examples of informational techniques are: strategic communication,[53] promulgating scientific research on disputed issues, public affairs, 'naming and shaming',[54] broadcast media venues for diaspora, framing of information by spokespersons or social media, abundant dissemination or withholding of information, advocating the influencers ideology, fake news, disinformation, lies, deterrence by disclosure,[55] propaganda,[56] and mal-information. Influence operations and information operations[57] are sometimes used interchangeably;[58] which is an approach that will not be followed in this thesis. In the literature information operations refer to two aspects: on the one hand there are the more technical activities to disrupt and disable the entire flow of information, including the ICT infrastructure they run on. On the other hand, information operations affect the non-technical, cognitive aspects of information; in other words, they attempt "to influence perceptions by affecting the content

49 Lindsay Maizland, "China's Repression of Uyghurs in Xinjiang," *Council on Foreign Relations*, 2021.

50 J.R. Miller, "Residential Schools in Canada," *The Canadian Encyclopedia*, 2021.

51 Jeff Farlin, "Instruments of National Power: How America Earned Independence," 2014. p. 5. Or as McDougal and Feliciano, "International Coercion and World Public Order: The General Principles of the Law of War." p. 793 put it: when speaking about the 'ideological instrument' as it was referred to then: "The use of the ideological instrument commonly involves the selective manipulation and circulation symbols, verbal or non-verbal, calculated to alter the patterns of identification, demands and expectations of mass audiences in the target-state and thereby to induce or stimulate politically significant attitudes and behavior favourable to the initiator-state."

52 Daniel Cohen and Ofir Bar'el, "The Use of Cyberwarfare in Influence Operations," *Blavatnik Interdisciplinary Cyber Research Center*, 2017. p. 8, Cohen and Bar'el refer to perception warfare in this sense.

53 Stephens, "Influence Operations & International Law."p. 3; Anaïs Reding, Kristin Weed, and Jeremy J. Ghez, "NATO's Strategic Communication Concept and Its Relevance for France," *RAND Publications*, 2010. p. 7.

54 Martha Finnemore and Duncan B. Hollis, "Beyond Naming and Shaming: Accusations and International Law in Cybersecurity," *European Journal of International Law* 31, no. 3 (2020): 969–1003. pp. 1002-1003.

55 The 2013 Snowdon leaks disclosing information collected by US National Security Agency and the UK Government Communication Headquarters, as well as the disclosure of Stuxnet probably gained the US and the UK some benefits in general deterrence. See: Gartzke and Lindsay, "Thermonuclear Cyberwar." p. 42.

56 Propaganda can be described as communication to shape attitudes and behaviour for political purposes. Propaganda can be persuasive and manipulative, but it can also be coercive if "the audience's choice of alternatives (is) severely restricted", See B S Murty and Harold D Lasswell, *Propaganda and World Public Order : The Legal Regulation of the Ideological Instrument of Coercion* (New Haven [etc.] SE - xiv, 310 p. ; 24 cm.: Yale University Press, 1968). pp. 1 & 129.

57 Tom Wilson, Kaitlyn Zhou, and Kate Starbird, "Assembling Strategic Narratives: Information Operations as Collaborative Work within an Online Community," *Proceedings of the ACM on Human-Computer Interaction* 2, no. CSCW (2018). p. 3.

58 Pontus Winter, "Military Influence Operations," 2017. & Larson et al., *Foundations of Effective Influence Operations*. & Jen Weedon, William Nuland, and Alex Stamos, "Information Operations and Facebook," *Facebook*, 2017, 1–13. p. 5.

of information",[59] with "the purpose of manipulating public opinion".[60] For the purpose of this research influence operation solely refer to the second (cognitive) notion.
Using the informational instrument of power to affect the cognitive dimension is also an element of RF influence activities. The RF focuses on the informational instrument of power, with the purpose of altering the understanding and decision-making process of targeted audiences, making use of events within other remits,[61] such as the distribution of energy or gas to and via the Ukraine. The energy dispute with Ukraine is used as an informational tool to underscore the unreliability of Ukraine and 'sow doubt about the wisdom of Ukraine as a NATO or EU member'.[62] Other opportunistic examples of the use of media outlets such as Russia Today (RT) as 'a wing of the government information team',[63] are the downing of the MH17 in 2014,[64] the 2015 Panama Papers,[65] the 2015 Syrian refugee crisis,[66] and the 2016 Lisa case.[67]

Though State A is able to use all the instruments of power, the specificities of influence operations imply that these instruments cannot be used in full. Diplomatic, informational and economic threats are included while the threat of the use of force is not. The characteristics of cyberspace as a domain of engagement further limit the use of instruments. Influence operations in or via cyberspace can make use of diplomatic (persuasive) means, but largely rely on the informational instrument of power with the aim to alter or undermine the deliberate understanding and autonomous decision-making of the targeted audience.[68]

59 Freedman, *The Future of War: A History*. p. 227; Weedon, Nuland, and Stamos, "Information Operations and Facebook."Weedon,), p. 5. Information Operations are also referred to as politically motivated operations, entailing actions to distort domestic or foreign political sentiment; See also: Stephens, "Influence Operations & International Law." p. 2.

60 Henning Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law," *Israel Law Review* 53, no. May (2020): 189–224. p. 193.

61 Collins, "Russia's Use of the 'Energy Weapon' in Europe."; Mason Richey, "Contemporary Russian Revisionism: Understanding the Kremlin's Hybrid Warfare and the Strategic and Tactical Deployment of Disinformation," *Asia Europe Journal* 16, no. 1 (2018): 101–13. pp. 103-105.

62 Richey, "Contemporary Russian Revisionism: Understanding the Kremlin's Hybrid Warfare and the Strategic and Tactical Deployment of Disinformation." p. 107.

63 Mona Elswah and Philip N. Howard, "'Anything That Causes Chaos': The Organizational Behavior of Russia Today (RT)," *Journal of Communication* 70, no. 5 (2020): 623–45. p. 636.

64 Kragh and Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case." pp. 788; Richey, "Contemporary Russian Revisionism: Understanding the Kremlin's Hybrid Warfare and the Strategic and Tactical Deployment of Disinformation." p. 102.

65 Benjamin Jensen, Brandon Valeriano, and Ryan Maness, "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist," *Journal of Strategic Studies* 42, no. 2 (2019): 212–34. p. 222.

66 Elswah and Howard, "'Anything That Causes Chaos': The Organizational Behavior of Russia Today (RT)." pp. 635-636.

67 Aristedes Mahairas and Mikhail Dvilyanski, "Disinformation – (Dezinformatsiya)," *The Cyber Defense Review*, 2018, 21–27. pp. 23-24.

68 Paul A.L. Ducheine and Peter B.M.J. Pijpers, "The Notion of Cyber Operations," in *Research Handbook on International Law and Cyberspace (Forthcoming)*, ed. Nicholas Tsagourias and Russell Buchan, 2nd ed. (Edward Elgar, 2021). pp. 7-10.

Given the aim to alter the cognitive dimension of State B via changing or undermining its deliberate understanding and autonomous decision-making process, influence operations use a clear strategic and calibrated[69] narrative as the exponent of the informational instrument of power.[70] Though not unique to cyberspace,[71] narratives are deliberate ways to influence audiences with the aim to persuade, manipulate and compel other States or State actors and thereby initiate the process of altering or counterbalancing the perceptions and belief and subsequently the context and weighing of the decision-making options, by using threats if necessary.

The strategic narrative is a cognitive construct that explains the world and shapes perceived interests[72] to unite groups of people,[73] generating a shared view of a collective history, culture, societal values[74] and a desired objective for the future.[75] Strategic narratives set the template to shape ideas, disseminate opinions and propagate favourable positions.[76] It also magnifies or undermines the shared attitude, identities and ways of communication of social entities.[77] A narrative needs to be clear, realistic and compelling, but also needs to be perceived as legitimate.[78] Order, consistency, style, language, and repetition of the message are pivotal.[79] Strategic narratives can make use of inherent and existing discourses within societies[80] to inject (counter) narratives in an opposing political system with the aim to unite and inspire specific people or groups (minorities or diaspora) to undermine the incumbent government, sow social discord, or exacerbate existing divisions in society.

69 Jeangene Vilmer, "Information Manipulation: A Challenge for Our Democracies." p. 75.

70 Wilson, Zhou, and Starbird, "Assembling Strategic Narratives: Information Operations as Collaborative Work within an Online Community." p. 4.

71 H. Porter Abbott, *The Cambridge Introduction to Narrative*, *Cambridge Introductions to Literature*, 2nd ed. (Cambridge: Cambridge University Press, 2008). pp. 13-15.

72 Laura Roselle, Alister Miskimmon, and Ben O'Loughlin, "Strategic Narrative: A New Means to Understand Soft Power," *Media, War and Conflict* 7, no. 1 (2014): 70–84. p. 76.

73 George Dimitriu and Beatrice De Graaf, "Fighting the War at Home: Strategic Narratives, Elite Responsiveness, and the Dutch Mission in Afghanistan, 2006-2010," *Foreign Policy Analysis* 12, no. 1 (2016): 2–23. pp. 7-8; Narratives are an element of strategic communication, whereby the latter is 'is not only about sending messages, but also about repeating and retelling them continuously, engaging in dialog, and building a net of relationships around them.' See also: Freedman, *The Future of War: A History*. p. 228.

74 Brick, "The #Future of War and the Fight for the Strategic Narrative." p. 1.

75 Dimitriu and De Graaf, "Fighting the War at Home: Strategic Narratives, Elite Responsiveness, and the Dutch Mission in Afghanistan, 2006-2010." p. 6.

76 Filippo Tansino, "Analysing Strategic Communications through Early Modern Theatre," *Defence Strategic Communications* 6 (2019): 38. p. 52.

77 George Lakoff, *The Political Mind: A Cognitive Scientist's Guide to Your Brain and Its Politics* (Penguin, 2009). pp. 232-241.

78 Abbott, *The Cambridge Introduction to Narrative*. p. 14; Dimitriu and De Graaf, "Fighting the War at Home: Strategic Narratives, Elite Responsiveness, and the Dutch Mission in Afghanistan, 2006-2010." p. 7.

79 Johan E. Korteling, Maaijke Duistermaat, and Alexander Toet, "Subconscious Manipulation in Psychological Warfare," 2018. pp. 35-38.

80 Tansino, "Analysing Strategic Communications through Early Modern Theatre." p. 55; Hutchinson, "Influence Operations: Action and Attitude." p. 13.

Narratives can be strategically used to sway targeted audiences.[81] The effectiveness of the narratives of a State is dependent on the possibility to coordinate, align and synchronise the instruments of power with other actors,[82] including NGOs, (state-controlled) media,[83] or international cooperation. Depending on the ideology and organisation of the political system these actors can be aligned with, or counterbalance, the instruments of power of the political system itself. Most liberal democracies have limited to no control over the media outlets,[84] and civil society is often far removed from being passive, pacified, or apolitical. In the RF there is a different situation altogether. There political elites provide leverage to pursue a centralised, consistent and State-controlled strategic narrative.[85] Cohen argues that there is a 'basic asymmetry in rules of engagement when conducting influence operations' between non-Western entities (including the RF or non-State ISIS) and liberal democracies. The latter adhere to laws and are marked by 'domestic disagreements that prevent the formulation of a uniform message'.[86] The open, transparent and competitive elections, freedom of speech, press freedom and free flow of information which are the strengths of liberal democracies can also be exploited as weaknesses.

Related to the RF intent to create strategic confusion in Western democracies,[87] the generic narratives used relate to the anti-EU,[88] anti-NATO and/or the 'anti-liberal democracy' sentiments,[89] based on feelings of increased Western Russophobia rife in the RF.[90] The RF

81 Roselle, Miskimmon, and O'Loughlin, "Strategic Narrative: A New Means to Understand Soft Power." pp. 74-75.

82 Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law." p. 195.

83 Such as RT or Sputnik in the Russian remit. See: Maria Hellman and Charlotte Wagnsson, "How Can European States Respond to Russian Information Warfare? An Analytical Framework," *European Security* 26, no. 2 (2017): 153–70. pp. 155-157.

84 Media Ajir and Bethany Vailliant, "Russian Information Warfare : Implications for Deterrence Theory," *Strategic Studies Quarterly*, 2018, 70–89. pp. 77-79.

85 Kragh and Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case." pp. 775-777; United States Senate Committee on Foreign Relations, "Minority Report on Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security," 2018. pp. 24 ff; Johana Evelyn Montalvan Castilla and Christer Pursiainen, "Cyberspace Effects on Civil Society. The Ultimate Game-Changer or Not?," *Journal of Civil Society* 8689 (2019). pp. 404-407.

86 Cohen and Bar'el, "The Use of Cyberwarfare in Influence Operations." p. 10; United States Senate Committee on Foreign Relations, "Minority Report on Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security." pp. 17-23; Lucas Kello, *The Virtual Weapon and International Order* (New Haven [CT] SE - xi, 319 pages ; 25 cm: Yale University Press, 2017). p. 219.

87 Laura Rosenberger, "Making Cyberspace Safe for Democracy," *Foreign Affairs* 99, no. 3 (2020): 146–60. Rosenberger argues that "Russian actors typically manipulate information not to persuade others or spread a view or an ideology but to sow confusion and disruption. Their aim is to create the impression that truth does not exist, undermining trust and authority in democracies."; Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict*. p. 83.

88 Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict*. pp. 84-85; Karin von Hippel, "Axis of Disruption : Chinese and Russian Influence and Interference in Europe," 2020. p. 7.

89 Mandiant, "'Ghostwriter' Influence Campaign," 2020. p. 4; Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict*. pp. 27-28; Jeangene Vilmer, "Information Manipulation: A Challenge for Our Democracies." p. 78; Jean Baptiste Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem" (Council, Atlantic, 2019). p. 44.

90 Elswah and Howard, "'Anything That Causes Chaos': The Organizational Behavior of Russia Today (RT)." p. 633, which is also a reason the RF incepted the English-language international channel Russia Today in 2005, to explain Russia policies.

strategic narrative is described as zero-sum, nationalistic[91] or even revisionist,[92] aiming to restore Russia's greatness and power,[93] and hence to destabilise the West,[94] and is based on 'information confrontation'-activities.[95] The aim of information confrontation is to change the perception and public opinion of the opponent, either in an advantageous way towards the RF or in a disadvantageous way towards their own political leadership.[96] The perception of the opponent - especially its population and leadership - is shaped via subversion and deception whereby the opponent is often unaware of the subconscious RF operation that paralyses its deliberate understanding and autonomous decision making.

In the next three sections the operationalisation and 'weaponizing' of the instruments of power, more specifically the strategic narrative, will be elaborated whereby the following queries will be addressed: how can cyberspace be used to employ the (informational) instruments of power of the State (§ 2.2.3); why is the audience susceptible to influence operation in cyberspace (§ 2.2.4); what cyber-related activities are used to target the audience in order to achieve effects (§ 2.2.5).

2.2.3. The domain of engagement

The engagement area is the operational environment where State A – the author State - and the targeted State B meet, communicate or fight. The 'arena' where two opposing actors meet can be a physical battlefield on land, in the air, or at sea, but influence operations in cyberspace solely engage in or via cyberspace.[97]

Cyberspace has its limitation. Not all instruments of power can be used since the (digital) form of cyberspace is not fit for all functions.[98] Nevertheless, form does not only follow function,

91 Ajir and Vailliant, "Russian Information Warfare : Implications for Deterrence Theory." p. 70.

92 Richey, "Contemporary Russian Revisionism: Understanding the Kremlin's Hybrid Warfare and the Strategic and Tactical Deployment of Disinformation." p. 103.

93 Kello, *The Virtual Weapon and International Order*. p. 218.

94 Ajir and Vailliant, "Russian Information Warfare : Implications for Deterrence Theory." pp. 70-71.

95 Iona Allan, Leonie Haiden, and Anna Reynolds, eds., *Fake News. A Roadmap*, 2018. pp. 61-62. In Western literature this is also translated as information warfare, see: Giles, "Handbook of Russian Information Warfare." p. 6; Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict*. p. 73.

96 Kragh and Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case." p. 778. Other narratives are American Exceptionalism', or the notion of the Israeli 'Promised Land'. See also: David Levering Lewis, "Exceptionalism's Exceptions: The Changing American Narrative," *Daedalus* 141, no. 1 (2012): 101–17. p. 108.

97 Michele Flournoy and Michael Sulmeyer, "Battlefield Internet: A Plan for Securing Cyberspace," Foreign Affairs, no. September/ October (2018). p. 1. The authors state that "Cyberspace has been recognized as a new arena for competition among States ever since it came into existence".

98 Marshall McLuhan, *Understanding Media: The Extensions of Man*, *International Journal of McLuhan Studies*, 1994. pp. 7-11; Peter B.M.J. Pijpers, "De Twitterende Tegenstander," *Militaire Spectator* 183, no. 6 (2014): 300–314. p. 303.

function also follow form[99] in the sense that cyberspace offers very specific characteristics that (re)shape communication channels, whether these are language, images, bullets or bytes.[100]

Cyberspace also generates unprecedented new opportunities due to its characteristics. Two elements will be elaborated on here: cyberspace as an additional means of communication and engagement (§ 'new vector'), and the production and disclosure of large sets of data (§ 'abundance of information'), which result in three emerging trends in which cyberspace can enhance and exploit influence operations (§ 'resulting trends').

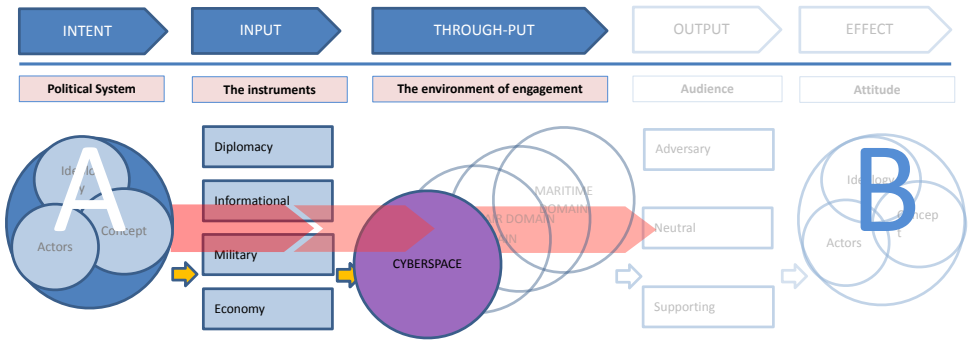

Figure 2 - 4 The engagement area

2.2.3.1. *New vector*

Cyberspace is a new man-made domain for engagement, which entails part of the physical and the entire virtual dimension. The physical network layer consists of hardware (computers, routers, smartphones) that stores and processes data and makes the transmission of data possible. This layer is present in the physical world and can suffer physical damage and destruction. All physical laws apply to this layer. The virtual dimension consists of the virtual persona and the logical layer. Virtual personae allow real persons or organisations to access cyberspace via e-mail addresses or accounts on social media platforms. The virtual personas

99 Corey Anton, "Media Ecological Orientations to Philosophy and Philosophical Problems," *Review of Communication* 17, no. 4 (2017): 224–39. p. 225. Based on the work of Neil Postman, Marshall McLuhan and Lewis Mumford, Corey Anton stated that: "*Not only do different environments and social places set the stage for likely and/or appropriate interaction, but also, less obviously, communication technologies become environments in their own right. Each medium, mode, or code of communication carries various kinds of biases, preferences for space, time, pace, and/or duration.*"

100 In the view of Marshall McLuhan 'media is the message' which means that our messages are shaped by the possibilities and limitations of our communication means. McLuhan, *Understanding Media: The Extensions of Man*. pp. 7-21. See also: Herbert S. Lin and Amy Zegart, eds., *Bytes, Bombs and Spies: Strategic Assessment of the US Cyber Command Vision* (Brookings Institution Press, 2019). pp. 6-9.

enable access to the logical layer, which includes all non-tangible elements manifested in data or codes ('zeros and ones'), such as operating systems, protocols, applications, or other software and data components.[101] Together with the physical network layer, the logical layer of software creates the Internet or 'electronic highway'.[102] Virtual elements of cyberspace may suffer functional damage and infringements of the confidentiality, integrity and availability of the system, but do not suffer real ill-effects or pass away nor do physical laws apply to the virtual world.

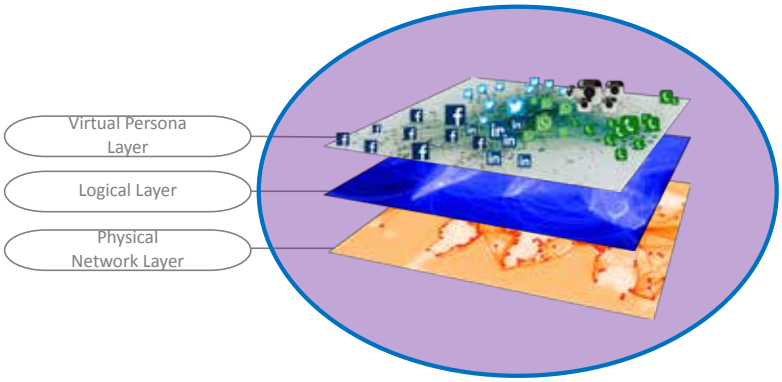

Figure 2 - 5 Cyberspace

Cyber operations can resort effect, either in cyberspace using cyberspace as a target, or outside, using cyberspace as a vector affecting the physical and cognitive layers of the information environment.[103] Stephens distinguishes cyber operations from influence operations. The former have the purpose of infiltrating cyber infrastructure with the aim to degrade capabilities, while the purpose of influence operations is 'to use existing infrastructure (especially social media) to engage in information, distortion, misinformation and or/ disinformation campaigns to proselytise specifically tailored politico-social messages so as to gain actual political and military advantage'.[104] The latter, influence operations, focus on the cognitive dimension of State B, the targeted State, but since direct targeting of the cognitive dimension is challenging, if not impossible, the instruments of power of the State will follow the path of the virtual or physical dimension of cyberspace.

101 Peter B.M.J. Pijpers and Kraesten L. Arnold, "Conquering the Invisible Battleground," *Atlantisch Perspectief* 44, no. 4 (2020). pp. 10-11.

102 See also § 1.2.1.

103 Betz and Stevens, "Power and Cyberspace." p. 41.

104 Stephens, "Influence Operations & International Law." p. 2.

On the basis of the categorisations made, activities in cyberspace can be divided in so-called hard-cyber and soft-cyber operations.[105] Hard-cyber operations aim to extract or modify data or cause denial of service[106] by deceiving, destroying or disclosing data, infrastructure or (virtual) persona.[107] Hard-cyber operations are cyber-related activities *in* cyberspace such as hacking a computer or disable, disrupt or destroy software. Examples of techniques used are severe DDoS attacks, hacking (intrusions of) databases of voters but also social engineering or spear phishing.[108] Soft-cyber operations are cyber-related activities *through* cyberspace that use cyberspace as a vector with the aim to target the cognitive dimension. Soft-cyber activities focus on the content of a message and the way it is disseminated, thereby also using techniques such as falsifying social media accounts.[109]

Influence operations as used in this research are inherently soft-cyber operations since they do not aim to affect the virtual or physical dimension of cyberspace. Their focus is on the content and the outlet (source) of a message with the aim to alter the deliberate understanding and autonomous decision-making process, hence the cognitive dimension. In reality, a sharp division between hard- and soft-cyber activities is difficult to uphold. Activities, such as doxing (hack-and-leak), combine hard- and soft-cyber operations.[110] Tampering with elections via cyberspace may also combine hard- and soft-cyber operations; the hardware of the voting machines can be disrupted or destroyed using malware,[111] while the voters are influenced via their profiles on social media.[112]

105 Pijpers and Arnold, "Conquering the Invisible Battleground." pp. 12-14; Paul A.L Ducheine and Jelle van Haaster, "Cyber-Operaties En Militair Vermogen," *Militaire Spectator* 182, no. 9 (2013). p. 378; A division between affecting the psyche and the materiel is not uncommon. The Russian doctrine mentions information-psychology and information-technology operations. See: Giles, "Handbook of Russian Information Warfare." p. 9; Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict*. pp. 3-4.

106 Sergio Castro, "Towards the Development of a Rationalist Cyber Conflict Theory," *The Cyber Defense Review* 6, no. 1 (2021): 35–62. p. 38.

107 Paul A.L. Ducheine, Jelle van Haaster, and Richard van Harskamp, "Manoeuvring and Generating Effects in the Information Environment," in *Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crisis - NL ARMS 2017*, ed. Paul A.L. Ducheine and Frans P.B. Osinga, 2017. pp. 2 & 15..; Kello, *The Virtual Weapon and International Order*. pp. 51-53.; Nye Jr., "Cyber Power." p. 6. Effects in cyberspace are a DDoS-attack, installing firewall, malware or malicious codes preparing an intellectual property theft. Effects though cyberspace include the disruption of SCADA control systems, and information campaign to sway voters' preferences.

108 Spear phishing is technique to disclose confidential information such as login credentials. These sophisticated techniques are tailored for specific persons and often use malicious emails which appear to be coming from colleagues or legitimate companies, see: Baezner and Robin, "Cyber and Information Warfare in Elections in Europe." p. 17.

109 Shires follows a similar distinction between cyber-enables information operations and cyber-assisted information operations. James Shires, "Hack-and-Leak Operations: Intrusion and Influence in the Gulf," *Journal of Cyber Policy* 4, no. 2 (2019): 235–56. p. 240; Nye Jr., "Cyber Power." pp. 2 & 5. Soft power behaviour rests on framing agendas, attraction or persuasion.

110 Ido Kilovaty, "Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information," *Harvard National Security Journal* 9 (2018): 146–79. p. 152.

111 Barrie Sander, "Democray under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections," *Chinese Journal of International Law*, no. December 2018 (2019). p. 6.

112 Jeangene Vilmer, "Information Manipulation: A Challenge for Our Democracies." p. 89. The definition of Social media is 'a form of electronic communication and networking sites that allows users to follow and share content and ideas within an online community' and follows the work of Thomas Zeitzoff, "How Social Media Is Changing Conflict," *Journal of Conflict Resolution* 61, no. 9 (2017): 1970–91. p. 1971.

2.2.3.2. *Abundance of information*

Apart from being a new vector, the added value of cyberspace lies in the ability to collect, select and subsequently unlock large amounts of information,[113] (user) data and knowledge with universal accessibility.[114] Cyberspace, including the Internet, is a 'repository' of facts and statistics, but also lies and innuendo that have not been and will not be checked or corroborated. Although they may evidently be fabricated and untrue, they will be given equal weight.[115] The characteristics of data and information in the virtual dimension, combined with the exploitation of social media,[116] can be used to influence targeted audiences in a persuasive, compelling and manipulative way. The effect is the interference or undermining of the control of the attitude and behaviour of citizens - including during democratic elections and the process of forming opinions on public policies.[117] Gorton argues that the use of big data strengthens and facilitates manipulative techniques,[118] and "to try to alter citizens' behaviour based on models of unconscious processes of the human mind".[119]

Cyberspace, and especially social media,[120] enhances the connectivity between large quantities of data sets.[121] These data include personal data which have been provided by individuals and groups using social media accounts on platforms such as Facebook.[122] Furthermore, traditional communication (oral and written) is one on one, while in mass media (TV/ pictorial) one outlet can influence many users. In cyberspace, social media networks influence each other,[123] meaning that many users communicate with many others, which empowers actors from non-State agencies to influence individuals. Cohen and Bar'el

113 Wilson, Zhou, and Starbird, "Assembling Strategic Narratives: Information Operations as Collaborative Work within an Online Community." pp. 3-4.

114 Made possible by increased processing power (Moore's law), miniaturization (Kryder's law) and de materialisation (Nielsen's law), see: Roy van Keulen, "Digital Force : Disrupting Life , Liberty and Livelihood in the Information" (2018). pp. 19-28.

115 James Ball, *Post-Truth: How Bullshit Conquered the World*, *Biteback Publishing* (London, 2017). p. 8.

116 Daniel Trottier and Christian Fuchs, "Theorising Social Media, Politics and the State: An Introduction," in *Social Media, Politics and the State: Protests, Revolutions, Riots, Crime and Policing in the Age of Facebook, Twitter and YouTube*, 2014, 3–38. pp. 14-16; Betz and Stevens, "Power and Cyberspace." pp. 50-52, referring to the 'productive cyber-power'.

117 Joseph S. Nye Jr., "Protecting Democracy in an Era of Cyber Information War," *Belfer Center*, 2019. p. 4.

118 William A. Gorton, "Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy," *New Political Science* 38, no. 1 (2016): 61–80. p. 62.

119 Gorton. p. 63

120 Federica; Liberini et al., "Politics in the Facebook Era. Evidence from the 2016 US Presidential Elections," 2018. p. 2.

121 House of Commons Digital Culture Media and Sport Committee, "Disinformation and 'Fake News': Final Report," 2019. Bullet 275, Chapter 3 on Data use and data targeting. Highlight mentioned on p. 41.

122 Information Commissioner's Office, "Investigation into the Use of Data Analytics in Political Campaigns," 2018. p. 17; Steven J Barela and Jérôme Duberry, "Understanding Disinformation Operations in the 21 St Century," in *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, ed. Jens David Ohlin and Duncan B. Hollis, 2021, 41–72. p. 55.

123 An example is the Russian use of so called "blacktivists" account to sow discord in the US. The idea is to launch numerous fake accounts and groups, the account that gain momentum will be populated while the neglected one's will serve to magnify or amplify the active accounts via bots and echo chambers. See also: Sam Levin, "Did Russia Fake Black Activism on Facebook to Sow Division in the US?," *The Guardian*, 2017.

argue that there is a shift from traditional dissemination via the media to the sharing of information by individuals and groups operating 'without a clear hierarchical model, and mostly lacking rules, regulation or government enforcement'.[124] Individuals do not simply receive messages, but 'social media allows these ordinary citizens to respond in kind', directly interact, and create their own content.[125] The indicator of its impact is not the authority of the media outlet as it was in the past, but the size of the network (Facebook, Twitter),[126] its mutual awareness, connectivity and the similarity between the users.[127]

2.2.3.3. Resulting trends

Trends emerging due to the character of cyberspace (new vector and the abundance of information) include undermining or inundating the public sphere,[128] micro-targeting, and enhancing predictive power without understanding.

Cyberspace unlocks the information environment and provides man-made tools to use and exploit that environment.[129] The information overload,[130] which is a result of that, offers choices to recipients of the data or to customers in a commercial setting. The overload of information and the lack of time to give significance to the available data also has the effect that groups or audiences are no longer able to make rational and deliberate choices[131] but are deflected to intuitive judgments based on cognitive and social heuristics. The ubiquitous presence of data may result in eroding and inhibiting the public dialogue, thereby manipulating the understanding and perception of targeted audiences.[132] The changes in society that commenced in the second half of the 20th century, related to deteriorating social and group loyalty, have led to more personalised politics away from collective values to a multitude of individual interests,[133] which is a trend that has intensified by the emergence

124 Cohen and Bar'el, "The Use of Cyberwarfare in Influence Operations." p. 8.

125 Zeitzoff, "How Social Media Is Changing Conflict." pp. 1972-1974.

126 Uta Kohl, "Jurisdiction in Cyberspace," in *Research Handbook on International Law and Cyberspace*, 2015, 30–54. p. 30.

127 Anatoliy Gruzd and Barry Wellman, "Networked Influence in Social Media: Introduction to the Special Issue," *American Behavioral Scientist* 58, no. 10 (2014): 1251–59. pp. 1255-1256.

128 Weedon, Nuland, and Stamos, "Information Operations and Facebook." p. 6. Facebook highlights the influence operation attempts making use of Facebook via three different techniques: targeted data collection; content creation; and false amplification. Targeted data collection Targeted data collection has the goal of stealing, and often exposing, non-public information that can provide unique opportunities for controlling public discourse.

129 Roetzel argues that 'the acquisition of information developed rapidly, the decision-maker's cognitive capacity did not', see: Peter G. Roetzel, "Information Overload in the Information Age: A Review of the Literature from Business Administration, Business Psychology, and Related Disciplines with a Bibliometric Approach and Framework Development," *Business Research* 12, no. 2 (2019): 479–522. p. 482.

130 Roetzel. p. 480.

131 Buster Benson, "Cognitive Bias Cheat Sheet, Simplified," *Medium*, 2017.

132 Gorton, "Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy." p. 69.

133 W. Lance Bennett, "The Personalization of Politics: Political Identity, Social Media, and Changing Patterns of Participation," *Annals of the American Academy of Political and Social Science* 644, no. 1 (2012): 20–39. pp. 37-38.

of cyberspace and, especially, social media.[134] The data available in cyberspace, more specifically on the Internet and social media, provide citizens with the possibility to filter out information that does not interest them or to ignore opinions with which they disagree. In a sense, social media – using automation, algorithms, and big-data analytics - are conducive to create 'echo chambers',[135] which magnify like-minded sources of information that can also be used for manipulative and polarising purposes.[136] The public sphere, as a platform for the public discourse and foundation of democratic systems,[137] could be further diminished by the possibility for groups of people to immerse in their own segment of the Internet via virtual and social media groups reflecting their own interest and beliefs,[138] potentially resulting in a fragmentation of the public agenda.[139] This 'group polarisation' violates one of the fundamentals of a well-functioning democracy, namely the shared experience.[140] Democracy requires independent and reliable news platforms, 'a pluralistic climate of opinion, and the ability to negotiate public consensus'.[141] After all, without common experiences a society cannot address social problems. A process that is subverted when social media are used to disseminate fabricated and false news manipulates public opinion.

Political micro-targeting, or micro-profiling is the ability to divide the population (voters) into very specific segments and customise messaging based on political preferences.[142] Social media provide a platform to audiences that might have lost the connection with the political mainstream.[143] Social media are said to be inducive to opposition actors in repressive

134 Ekaterina Zhuravskaya, Maria Petrova, and Ruben Enikolopov, "Political Effects of the Internet and Social Media," *SSRN Electronic Journal*, 2019, 1–32. p. 7, arguing that 'the spread of the internet and social media has contributed, at least in part, to the electoral success of populists in Europe and to reduced political support for the ruling parties in immature democracies and semi-autocratic regimes. There is also evidence that social media can be used to mobilize voters'.

135 Liberini et al., "Politics in the Facebook Era. Evidence from the 2016 US Presidential Elections." p. 7; Jens David Ohlin, *Election Interference: International Law and the Future of Democracy* (Cambridge University Press, 2020). p. 28.

136 For instance during the 2017 Catalan Reference where RT and Sputnik constantly framed the news headlines to sow discord and pointing to the negligence of the EU. David V. Gioe, "Cyber Operations and Useful Fools: The Approach of Russian Hybrid Intelligence," *Intelligence and National Security* 33, no. 7 (2018): 954–73. pp. 955-956; EU vs Disinformation, "Election Meddling and Pro-Kremlin Disinformation: What You Need to Know," 2019. p. 3.

137 Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law." p. 189.

138 Cass Sunstein, "The Daily We: Is the Internet Really a Blessing for Democracy?," Boston Review, 2001, http://bostonreview.net/cass-sunstein-internet-democracy-daily-we. p. 13.

139 Tom Dobber, "Data & Democracy: Political Microtargeting: A Threat to Electoral Integrity?" (University of Amsterdam, 2020). p. 113. In his research Dobber finds no direct evidence that political microtargeting for a fragmentation of the public agenda but suggests it should be measured over a longer time span.

140 Sunstein, "The Daily We: Is the Internet Really a Blessing for Democracy?" p. 6.

141 Philip N. Howard, John Kelly, and Camille François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018," *Computational Propaganda Research Project*, 2018. p. 39.

142 Howard, Kelly, and François. p. 39; Ohlin, *Election Interference: International Law and the Future of Democracy*. pp. 26-29; Dobber, "Data & Democracy: Political Microtargeting: A Threat to Electoral Integrity?" pp. 8-11; Dan Gizzi, "The Ethics of Political Micro-Targeting," The Medium, 2018, https://medium.com/datadriveninvestor/the-ethics-of-political-micro-targeting-c3b0be245607.

143 Philippe J. Maarek, "Politics 2.0: New Forms of Digital Political Marketing and Political Communication," *Trípodos* 1, no. 34 (2014): 13–22. pp. 18-19.

regimes.[144] Micro-targeting allows the formulation of personalized and propagated messages and their direct delivery to groups and individuals[145] by exploiting extensive quantities of user-generated data generated by social media.[146] Social media that use big data techniques i.e. mobile connectivity, algorithms and cloud computing,[147] are elementary as they grant access to the public data of a person (voter registration, location, age, gender) and consumer and lifestyle information (income, spending habits).[148] The rise of political micro-targeting can be explained due to the accessibility of voters via mobile applications, in-depth statistics generated via social media, and awareness that traditional mass messaging does not reach all voters.[149] The psychological profiling[150] and the micro-targeting based on that supports political outreach,[151] since the number of citizens' participation will increase due to micro-targeting, which strengthens democracy. However, it also creates threats since micro-targeting could invade privacy and manipulates voters' deliberations and choices by sending them bespoke and framed messages. Micro-targeting can even be used to 'increase apathy' and exclude groups by dissuading them to vote.[152] For political parties micro-targeting can be a cheap and effective way to reach specific voters, using form, context and language adjusted to a specific audience.[153] But more elaborate micro-targeting software, used for targeting the subconscious (heuristic or psychological) realm, as was offered by Cambridge Analytica, is expensive and unintentionally empowers these brokers.[154] For public opinion as such the benefit is that micro-targeting diversifies the public debate meaning that a campaign will

144 Zhuravskaya, Petrova, and Enikolopov, "Political Effects of the Internet and Social Media." p. 3.

145 Orestis Papakyriakopoulos et al., "Social Media and Microtargeting: Political Data Processing and the Consequences for Germany," *Big Data & Society* July-Dec (2018). p. 1.

146 Liberini et al., "Politics in the Facebook Era. Evidence from the 2016 US Presidential Elections." p. 37.

147 Ron Deibert, "The Geopolitics of Cyberspace," *Geopolitics*, 2009. p. 9.

148 Gorton, "Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy." p. 68; E.g. the 'OCEAN' five-factor model rating a personality on openness, conscientiousness, extraversion, agreeableness and neuroticism, as depicted in Christopher Wylie, *Mindf*ck: Cambridge Analytica and the Plot to Break America* (Random House, 2019). pp. 34-35.

149 Bennett, "Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications." pp. 372-378.

150 Ido Kilovaty, "Legally Cognizable Manipulation," *Berkeley Technology Law Journal* 34 (2019). pp. 465-466.

151 Dobber, "Data & Democracy: Political Microtargeting: A Threat to Electoral Integrity?" pp. 25-27. Dobber introduces Political Behaviour Targeting when social media not only facilitates new ways of communication, but tracks and collects behavioural data of Internet users; Maarek, "Politics 2.0: New Forms of Digital Political Marketing and Political Communication." pp. 19-20. As an illustration see: Wylie, *Mindf*ck: Cambridge Analytica and the Plot to Break America*. p. 22.

152 Hilder, "' They Were Planning on Stealing the Election ': Explosive New Tapes Reveal Cambridge Analytica CEO ' s Boasts of Voter Suppression ," no. January (2019). In Trinidad and Tobago, and Nigeria groups of (young) voters were discouraged to vote. But see also the Egyptian 2011 case in: Sara Salem, "Creating Spaces for Dissent: The Role of Social Media in the 2011 Egyptian Revolution," in *Social Media, Politics and the State: Protests, Revolutions, Riots, Crime and Policing in the Age of Facebook, Twitter and YouTube*, 2014, 171–88. pp. 180-186.

153 Matz cs argues that psychologically tailored advertising, including for political purposes, alters behaviour significantly if the content of persuasive appeals are matched with individuals' psychological characteristics. See: S. C. Matz et al., "Psychological Targeting as an Effective Approach to Digital Mass Persuasion," *Proceedings of the National Academy of Sciences of the United States of America* 114, no. 48 (2017): 12714–19. p. 12714

154 Kaiser describes a 5-phased approach of how Cambridge Analytica micro-targets audiences based on group preferences obtained via Facebook tools making use of the OCEAN- scores , see: Brittany Kaiser, *Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again* (Harper, 2019). pp. 85-87.

not focus on one topic, but on the other hand, diversification leads to fragmentation so that the overall political message will be lost.[155] Micro-targeting could potentially achieve 'instant influence (i.e.) trigger the person's mind to develop a conditioned response'[156] in accordance with what the influencer desires. This happens 'because in cases of fast incoming information stimuli, the individual does not process them rationally'.[157] The availability of big data and the attributes of cyberspace in general create ideal conditions for framing messages and executing disinformation and trolling operations, thereby infringing the free choice of targeted audiences.

The availability of big data and powerful algorithms also create the illusion of predictability of behaviour,[158] making use of 'hidden correlations amid the myriad data points."[159] Examples are the multiple regression techniques used by YouGov to predict elections polls, a marketing tool using answers of paid panellists on a wide range of (non-political) issues,[160] predicting elections results based on Twitter tags;[161] Facebook's Core Audience and Custom Audience's tool;[162] or the vector auto-regression comparison based on Twitter posts and retweets concluding that every 25,000 Tweets account for one percent change in the opinion polls.[163] Though these algorithm-based correlations do not reflect causality between the attitude and the behaviour of the voter, they do have an effect on voter preferences and voting behaviour,[164] partially due to the human inclination for sympathising or social belonging,[165] or related social heuristics.[166] These algorithms make use of computer science rather than social theory, resulting in 'prediction and control of voter behaviour without

155 Frederik J.Zuiderveen Borgesius et al., "Online Political Microtargeting: Promises and Threats for Democracy," *Utrecht Law Review* 14, no. 1 (2018): 82–96. pp. 84-92.

156 Papakyriakopoulos et al., "Social Media and Microtargeting: Political Data Processing and the Consequences for Germany." p. 10.; Robert B Cialdini, *Influence: The Psychology of Persuasion*, Rev. ed. (New York SE - xiv, 320 pages : illustrations ; 24 cm: Harper, 2007). pp. 273-280.

157 Papakyriakopoulos et al., "Social Media and Microtargeting: Political Data Processing and the Consequences for Germany." p. 10.

158 Stephan; Lewandowsky, John; Cook, and others, "The Debunking Handbook 2020," 2020. p. 5.

159 Gorton, "Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy." p. 72.

160 Chris Stokel-Walker, "How YouGov Became the UK ' s Best but Most Controversial Pollster," *Wired*, 2019.

161 Lei Wang and John Q. Gan, "Prediction of the 2017 French Election Based on Twitter Data Analysis," *2017 9th Computer Science and Electronic Engineering Conference, CEEC 2017 - Proceedings*, 2017, 89–93.

162 Allison Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign," *Boston University International Law Journal* 37, no. 171 (2019): 183–210. pp. 188-192.

163 Damian Ruck et al., "Internet Research Agency Twitter Activity Predicted 2016 U.S. Election Polls," First Monday, 2019, https://firstmonday.org/ojs/index.php/fm/article/view/10107/8049. Under Results: IRA Twitter success predicted election opinion polls, stating that: 'Overall, the effect is quantified such that a gain of 25,000 re-tweets per week over all IRA tweets (or about 10 extra re-tweets per tweet per week), predicted approximately one percent increase in Donald Trump's poll numbers.'

164 Liberini et al., "Politics in the Facebook Era. Evidence from the 2016 US Presidential Elections." pp. 37-38; see also examples of psychological warfare as used in Wylie, *Mindf*ck: Cambridge Analytica and the Plot to Break America*. pp. 40-55.

165 Cialdini, *Influence: The Psychology of Persuasion*. pp. 167 ff.

166 Korteling et al. argue that people are 'herd animals'. Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare." pp. 32-34.

understanding their views, values, needs, or desires."[167] Besides, an 'argument by analogy leads to conviction rather than to proof, and has often led to glaring error'.[168] Once algorithms based on computational science or even computational propaganda[169] are set, cyber-related activities such as disinformation campaigns can steer the behaviour of an audience based on heuristics. Using group biases, persons or groups receive content that was 'liked' by persons with similar background or preferences.[170] This system of 'clickbait'[171] induces groupthink and behaviour within virtual communities.[172]Thus, constantly repeating the content will appeal to the cognitive heuristic of retainment.[173] The framed disinformation campaigns with doctored, true or false content will become reality.[174]

Influence operations making use of disinformation campaigns during foreign elections, are not new, but the impact they can have by making use of cyberspace is. Executing influence operations in cyberspace and via social media facilitate their execution,[175] since the advance of digital technology allows the spread of (dis)information in large quantities and at high speed.[176] Though social media (or cyberspace) spread false news faster than genuine news,[177]

167 Gorton, "Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy." p. 73, see also M. Kosinski, D. Stillwell, and T. Graepel, "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior," *Proceedings of the National Academy of Sciences* 110, no. 15 (2013): 5802–5. p. 5804; see also: Roger Penrose, *AI, Consciousness, Computation and Physical Law*, 2019.

168 Winston S. Churchill, "The Scaffolding of Rhetoric," 1897.

169 Samuel C. Woolley and Philip N. Howard, "Political Communication, Computational Propaganda, and Autonomous Agents: Introduction," *International Journal of Communication* 10 (2016).

170 Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *The Journal of Slavic Military Studies* 17, no. 2 (2004): 237–56. p. 245; Humans are receptive for positive emotions, and 'Likes' induce and accelerate the hunger for this sentiment, see Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare." p. 31, who speaks about the 'hedonistic treadmill'; Yosh Halberstam and Brian Knight, "Homophily, Group Size, and the Diffusion of Political Information in Social Networks: Evidence from Twitter," *National Bureau of Economic Research*, 2014. p. 22.

171 Clickbait is a technique to lure social media users to spend more time on Internet (to increase the so-called 'time on site') by offering sensational cliff hangers (including lists). Though clickbaits spark curiosity they are usually fake and often divisive or partisan, see Richard Rogers and Sabine Niederer, eds., *The Politics of Social Media Manipulation* (Digital Methods Initiative, University of Amsterdam, 2019). pp. 1-6.

172 Jonatan C. Ong and Jason V.A. Cabanes, "Politics and Profit in the Fake News Factory - Four Work Models of Political Trolling in the Philippine," *NATO Strategic Communication Centre of Exellence*, 2019. pp. 17-20; Samantha Bradshaw and Philip N. Howard, "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation," 2018. p. 4.

173 As reflected in the so-called Thomas theorem stating that "if men define situations as real, they are real in their consequences". William I. Thomas and Dorothy S. Thomas, *The Child in America : Behavior Problems and Programs*, ed. Dorothy Swaine Thomas (New York: Knopf, 1928). p. 572. Repetition or multiple exposure of (dis)information is one of the techniques of retainment. A technique already used by Goebbels ('Wenn man eine große Lüge erzählt und sie oft genug wiederholt, dann werden die Leute sie am Ende glauben') but also used in the Lisa Case. See: Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare." p. 22.

174 Peter M. DeMarzo, Dimirti Vayanos, and Jeffrey Zwiebel, "Persuasion Bias, Social Influence, and Unidimensional Opinions," *The Quarterly Journal of Economics*, no. August (2003): 909–68. pp. 911-912.

175 Kello, *The Virtual Weapon and International Order*. p. 220; Marius Laurinavi, "A Guide to the Russian Tool Box of Election Meddling," 2018. p. 8.

176 Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict*. pp. 74-75.

177 Zhuravskaya, Petrova, and Enikolopov, "Political Effects of the Internet and Social Media." p. 18.

social media as such do not change the outcome of elections or polarise views and opinion.[178] It is an instrument that needs to be used properly to have an effect.

2.2.4. Targeting the audience

Influence operations are effective only if the targeted audience is susceptible to the content and rationale of the strategic narrative. Reaching the targeted audience can be facilitated by using the inherent dynamics within societies,[179] but also by using the heuristics and preferences of groups within that society. Heuristics set in once the boundaries of the rational decision-making process are reached. When planning for influence operations, the heuristics and socially divisive topics within a society can be used to frame the strategic narrative as a precursor to executing the cyber-related activities. Depending on how State A want to influence State B, the frame will be more or less persuasive, compelling or manipulative in nature.[180]

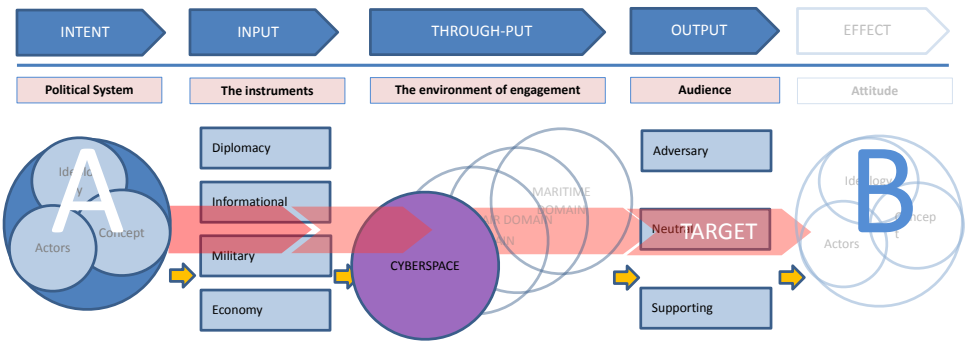

Figure 2 - 6 Targeting the audiences of State B

178 Zhuravskaya, Petrova, and Enikolopov. p. 14; Pablo Barberá, "How Social Media Reduces Mass Political Polarization . Evidence from Germany, Spain, and the U.S.," *LXXIII Congress of the Midwest Political Science Association*, 2014, 44. pp. 28-29.

179 Tansino, "Analysing Strategic Communications through Early Modern Theatre."; Thomas Elkjer Nissen, "#TheWeaponizationOfSocialMedia," 2015. pp. 43-44.

180 Peter B.M.J. Pijpers and Paul A.L. Ducheine, "Influence Operations in Cyberspace - How They Really Work," *Amsterdam Center for International Law* 61 (2020). pp. 6-9.

2.2.4.1. *Communication Dynamics*

Shared practices, ideas and values are not fixed but in a State of continuous change.[181] If there are tensions or conflicts people will communicate[182] in order to achieve or influence a common view and shared representation,[183] examples of which are the paradoxical dichotomy between health and economy in the age of Covid-19,[184] or topics regarding police violence, gender (in)equality, and immigrants' rights. Influence operations of State A will use these inherent antagonistic dynamics within societies based on contrasting views, values and opinions of groups and of the political leadership or population.

The essence of socially divisive topics, especially for democracies, is that these topics force groups in society to communicate,[185] in order to crystallise views and generate a shared representation of the facts and the context,[186] whether during election time, ad-hoc rallies or on late night talk shows.

The socially divisive topics can be linked to specific audiences or allotted to them based on thorough demographic research. States have specific societal divisions, which stem from different languages used in a State, differences in economic progress in the various regions of that State, or political views ranging from liberal to conservative, and based on urban or rural perspectives.[187] Societal divisive topics, whether existing or created, can be linked to the existing differences or occurrences, thereby generating or increasing the gap between groups and sowing discord. The UK referendum on sustained EU membership became linked to migration issues, economic malaise and declining healthcare which are issues not directly related to the UK membership of the EU.[188]

181 Moscovici, "The history and actuality of social representations", in Uwe Flick, ed., The Psychology of the Social (Cambridge, UK [etc: Cambridge University Press, 1998). pp. 209-47.

182 Elizabeth R. Nugent, "The Psychology of Repression and Polarization," *World Politics*, 2020. p. 11; Or paraphrasing Moscovici: "there would be hardly any reason to communicate if there were no tensions, asymmetries or conflicts between interacting parties", in Tansino, "Analysing Strategic Communications through Early Modern Theatre." p. 54.

183 Tansino, "Analysing Strategic Communications through Early Modern Theatre." p. 53. Paraphrasing Moscovici who argues that there are three communicative needs within any social group: the need to make a foreign element familiar, the need to create a shared field of communication, and the need to form a common identity.

184 Kristalina Georgieva and Tedros A. Ghebreyesus, "Some Say There Is a Trade-off : Save Lives or Save Jobs – This Is a False Dilemma," International Monetary Fund, 2020.

185 Nugent, "The Psychology of Repression and Polarization." p. 11; Or paraphrasing Moscovici: "there would be hardly any reason to communicate if there were no tensions, asymmetries or conflicts between interacting parties", in Tansino, "Analysing Strategic Communications through Early Modern Theatre." p. 54.

186 Tansino, "Analysing Strategic Communications through Early Modern Theatre." p. 53. Paraphrasing Moscovici who argues that there are three communicative needs within any social group: the need to make a foreign element familiar, the need to create a shared field of communication, and the need to form a common identity.

187 An in-depth study on social cleavages in Western Europe was conducted by Jan-Erik Lane and Svante O. Ersson, *Politics and Society in Western Europe*, 4th ed. (Sage Publications , Inc, 1999). pp. 37 ff, which relates to earlier work by Almond, see: Gabriel A. Almond, "Comparative Political Systems," *The Journal of Politics* 18, no. 3 (1956): 391–409.

188 Ece O. Atikcan, Richard Nadeau, and Eric Belnager, *Framing Risky Choices: Brexit and the Dynamics of High-Stakes Referendums* (McGill-Queen's University Press, 2020). pp. 50-52

Socially divisive topics address the cognitive dimension of the targeted audience, but still represent a very conscious way of persuading an audience using arguments, logic and rationale. This might still not make an audience instantly receptive to alter its understanding or better still, change its behaviour. To achieve that, the influence operation must either be more compelling - using threats - or circumvent the understanding and decision-making altogether in a deceptive manipulative influence operation, in which the subconscious cognitive processes of groups and audiences are addressed.[189]

2.2.4.2. *Cognitive limitations*

Aside from but complementary to the internal dynamics in society, influence operations can make use of the cognitive limitations of the rational decision-making process.[190] The rational mind of humans has its boundaries. Rational and analytical deliberations benefit from strong, relevant, consistent arguments and the availability of data. Processing this information will take time and effort[191] as the receiver will need to digest and internalise the arguments before a change of belief or perception will be achieved.[192]

The rational decision-making process can be impaired by manipulations related to time[193] and information.[194] It can also be diminished by the inability to give significance to data due to scarcity or a surge of information, a limited time slot to make a decision, or even the burden of memory (prior knowledge).[195] These cognitive limitations[196] may result in a deflection towards the application of social and cognitive heuristic which invokes a subconscious manner of processing information.[197] Although heuristics normally result

189 Bouwmeester, *Krym Nash: An Analysis of Modern Russian Deception Warfare*. pp. 158-165.

190 Herbert A. Simon, *The Sciences of the Artificial*, 3nd ed. (Cambridge, Mass. ; The MIT Press, 1996). Chapter 2 as of p. 25. Simon refers to these limits are 'bounded rationality', see p. 38 and on; Daniel Kahneman, *Thinking, Fast and Slow* (London [etc: Penguin, 2012). pp. 13-15 & part II on heuristics and biases.

191 Alexander; Toet et al., "Effects of Personal Characteristics on Susceptibility to Decision Bias : A Literature Study," *International Journal of Humanities and Social Sciences*, no. November (2016). p. 4.

192 Without stating that there is a causal relation between a change in attitude and a change in behaviour. The relationship, correlation or causality between attitude and behaviour is contested in literature, see: Jonas Dalege et al., "Toward a Formalized Account of Attitudes: The Causal Attitude Network (CAN) Model," *Psychological Review* 123, no. 1 (2016): 2–22. p. 3.; Joop van der Pligt and Michael Vliek, *The Psychology of Influence : Theory, Research and Practice* (London: Routledge, 2017). pp. 18-23.

193 Wood argues that pressurising is a form of manipulation. Allen W. Wood, "Coercion, Manipulation, Exploitation," in *Manipulation : Theory and Practice*, ed. Christian Coons and Michael Weber (Oxford University Press, 2014). p. 35.

194 Kahneman, *Thinking, Fast and Slow*. pp. 36-38.

195 Leon Festinger, *A Theory of Cognitive Dissonance* (Stanford University Press, 1985). pp. 260-266; Buster Benson, "Cognitive Bias Cheat Sheet," *Better Humans*, 2016.

196 Toet et al., "Effects of Personal Characteristics on Susceptibility to Decision Bias : A Literature Study." p. 3.

197 Pligt and Vliek, *The Psychology of Influence : Theory, Research and Practice*. pp. 61 & 80.

in acceptable outcomes in everyday situations, they certainly deviate from rationality and logic.[198]

Based on this, a division can be made between using conscious avenues of influencing and subconscious ones. Korteling et al. argue that 'persuasion and decision making can be accomplished either through a more conscious and deliberate route or through a more subconscious, intuitive processing route',[199] whereby the 'subconscious, intuitive processes are irrational or heuristic: this means that they do not involve deliberate analysis and calculation'.[200] The conscious and subconscious process is known in literature as the dual process model.[201] Others have similar 'dual' models: Pligt makes a difference between the persuasion by argumentation and the cognitive and social heuristics;[202] Allcott argues that people (voters), on the one hand, want to know the truth about a topic or candidate but, on the other, they are compelled to 'derive psychological utility' from data that comply with their preferences;[203] Moscovici makes a difference between instrumental and symbolic communication, hence between *what* is expressed and *how* it is expressed,[204] referring to the social and cognitive inclinations of an audience.

Social and cognitive heuristics are ingrained and universal mental mechanisms of humans and groups of humans.[205] The heuristics themselves cannot easily be used to influence, therefore the tools of influence will focus on invoking the reflexes towards these heuristics i.e. limits in time, overload of information and the subsequent inability to give meaning to the provided data.[206] Other tools of influence which may invoke the heuristics are

198 Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science* 185, no. 4157 (1974): 1124–31. p. 1131; Johan E. Korteling, Anne-Marie Brouwer, and Alexander Toet, "A Neural Network Framework for Cognitive Bias," *Frontiers in Psychology* 9 (2018). p. 2.

199 Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare." p. 8; Barfman and Barfman refer to the subconscious as the derailing of rational thinking which sways to irrational behaviour. Ori Barfman and Rom Barfman, *Sway: The Irresistible Pull of Irrational Behaviour* (Ebury Publishers, 2009). p. 7.

200 Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare." p. 9.

201 Pligt and Vliek, *The Psychology of Influence : Theory, Research and Practice*. P. 23.; Kahneman, *Thinking, Fast and Slow*. pp. 21-24.; Richard E Petty and John T. Cacioppo, *Attitudes and Persuasion: Classic and Contemporary Approaches*, ed. John T Cacioppo, *Attitudes and Persuasion*, [New ed.] (Boulder: Westview Press, 1996).; Toet et al., "Effects of Personal Characteristics on Susceptibility to Decision Bias : A Literature Study." p. 4.; Herbert Lin, "The Existential Threat from Cyber-Enabled Information Warfare," *Atomic Scientists* 75, no. 4 (2019): 187–96. pp. 8-11. The dual model could be traced back to Aristotle's differentiation between persuasion involving emotion versus reason. See also: Richard E Petty and Pablo Briñol, "Persuasion: From Single to Multiple to Metacognitive Processes," *Association for Psychological Science* 3, no. 2 (2008): 137–47. p. 138.

202 Pligt and Vliek, *The Psychology of Influence : Theory, Research and Practice*. pp. 39, 58, 77. Though the division between the two elements of the dual system – conscious and subconscious decisions and judgments is made for academic purposes, in reality these are inseparable.

203 Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election," *Journal of Economic Perspectives* 31, no. 2 (2017): 211–36. p. 218.

204 Serge Moscovici and Patricia Neve, "Studies in Social Influence. II: Instrumental and Symbolic Influence," *European Journal for Social Psychology* 3, no. 4 (1974): 461–71. pp. 461-462.

205 Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare." p. 4.

206 Benson, "Cognitive Bias Cheat Sheet, Simplified."

psychological tools including the OCEAN-personality test[207] used by Cambridge Analytica,[208] or the use of computational and social network influencing that invokes heuristics based on algorithmic correlations.[209]

2.2.4.3. Ways of influence

In this research influence operations are deliberate activities targeting the cognitive dimension in order to change attitude or behaviour.[210] Making use of communicative dynamics in societies and the cognitive limitations of groups in that society and excluding the threat or use of force results in three forms of influence, namely persuasion, compellence,[211] and manipulation.[212]

Persuasive but also compelling influence operations make use of techniques that openly appeal to the 'conscious deliberation'[213] of the targeted audience rather than on their cognitive limitations. Persuasive influence operations aim to alter the perception and worldview – the attitude[214] – of the targeted audience of State B. in an often overt, persuasive way, in order to change State B's understanding of the environment. By changing the weighing of the options to choose from persuasive influence operations can subsequently impact the autonomous decision making of the targeted audiences,[215] (State leadership, opinion leaders, mass public),[216] changing the behaviour of State B accordingly in a way advantageous

207 James Ball, "The Real Story of Cambridge Analytica and Brexit," *The Spectator*, 2020. Ocean is the acronym for openness, conscientiousness, extraversion, agreeableness and neuroticism. See also § 2.2.3.3.

208 Kaiser, *Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again*. pp. 84-85.

209 Woolley and Howard, "Political Communication, Computational Propaganda, and Autonomous Agents: Introduction."

210 Pijpers and Ducheine, "Influence Operations in Cyberspace - How They Really Work." p. 9.

211 Daniel Susser, Beate Roessler, and Helen Nissenbaum, "Online Manipulation: Hidden Influences in a Digital World," *Georgetown Law Technology Review* 4, no. 1 (2019): 1–52., pp. 13-17. For the purpose of this thesis the term 'compellence' is used to influence behaviour in general. Coercion will be associated to compelling acts of influence in a legal setting, see Chapter 3.

212 The categorisation is based on Ido Kilovaty, "The Elephant in the Room: Coercion," *AJIL Unbound* 113, no. June 27 (2019): 87–91. p. 88; Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Second ed. (Cambridge, United Kingdom ; SE - xli, 598 pages ; 24 cm: Cambridge University Press, 2017). pp. 381 ff; Jelle van Haaster, "On Cyber: The Utility of Military Cyber Operations During Armed Conflict" (2018). pp. 33-36; Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law." pp. 190-192. But the division can be traced back to the writings of Plato (Apology, Crito) as pointed out by Arendt in: Arendt, "Philosophy and Politics." pp. 427-432.

213 Susser, Roessler, and Nissenbaum, "Online Manipulation: Hidden Influences in a Digital World." p. 14.

214 The most common target of persuasion is a person's attitude. The latter being the primary object of influence due to their presumed influence on choices and action, thus Petty and Briñol, "Persuasion: From Single to Multiple to Metacognitive Processes." p. 137.

215 Susser, Roessler, and Nissenbaum, "Online Manipulation: Hidden Influences in a Digital World." p. 14; Chong and Druckman argue that 'an attitude toward an object is the weighted sum of a series of evaluative beliefs about that object'. Dennis Chong and James N. Druckman, "Framing Theory," *Annual Review of Political Science* 10 (2007): 103–26. pp. 104-105.

216 Duncan B. Hollis, "The Influence of War; The War for Influence," *Temple International and Comparative Law Journal* 32, no. 1 (2018): 31–46. pp. 35-36.

to the influencer.[217] Persuasive influence operations entail an open appeal to rational and a conscious deliberation. The essence is that the targeted audience retains, or perceives to retain, the ability to make a conscious and 'willing' choice,[218] based on meaningful options, to alter its attitude and behaviour,[219] hence to act or not to act.

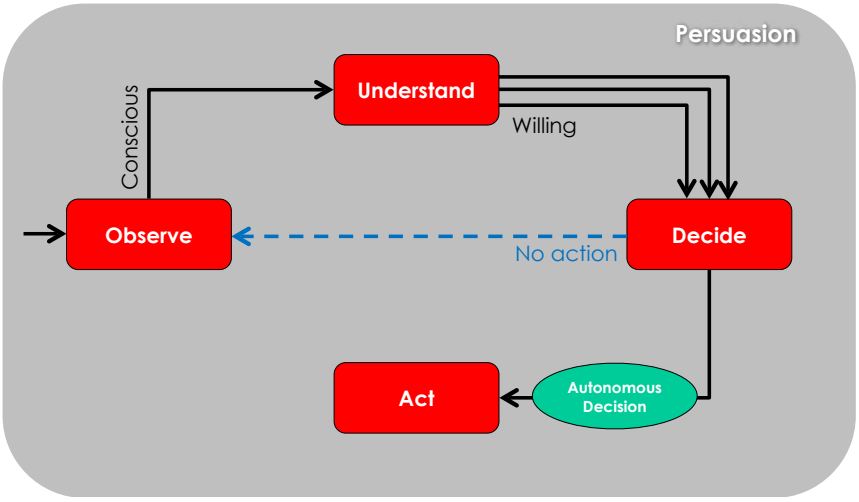

Figure 2 - 7 Conscious Persuasive Influence Operation

Persuasion is a normal rhetorical tool with which facts and reasons are presented in a 'fair and neutral way'.[220] Persuasion, therefore, is speech without compulsion.[221] Changing the political system of State B with persuasive means of influence is challenging since both the ideology and the concept (design) of the political system are not prone to regular change. A change in the belief system will require a 'high degree of thought',[222] as the arguments need to be accepted or internalised.[223] Persuasive influence operations are therefore time-consuming and require deliberate, sustainable and conscious discussion and exchange of

217 See also, Herbert Lin and Jackie Kerr, "On Cyber-Enabled Information / Influence Warfare and Manipulation," in *Oxford Handbook of Cybersecurity (Forthcoming)*, 2019, 1–29. p. 6.

218 Hollis, "The Influence of War; The War for Influence." p. 36; Lin and Kerr, "On Cyber-Enabled Information / Influence Warfare and Manipulation." p. 5.

219 Hollis, "The Influence of War; The War for Influence." p. 36. A persuasive influence operation is aligned with Hollis' influence operations which exclude coercion.

220 Cass R. Sunstein, "Fifty Shades of Manipulation," *Behavioral Marketing*, 2015. p. 216.

221 Persuasion and rhetoric were the highest form of political art to the ancient Greek, see: Arendt, "Philosophy and Politics." p. 427.

222 Pligt and Vliek, *The Psychology of Influence : Theory, Research and Practice*. p. 23.

223 Petty and Briñol, "Persuasion: From Single to Multiple to Metacognitive Processes." p. 138.

views.[224] Persuasive influence operations will often coalesce with activities of the diplomatic instrument of power. The long-term endeavour is required not least since State B is inherently motivated to support the existing ideology and concept of the State that has been sustained for a considerable period of time.[225] However, if successful, the changes obtained by persuasive influence operations will be long-lasting.[226]

Compelling influence operations can be explained in terms of a conscious but unwilling act.[227] Compelling operations do not provide meaningful options to the opposing audience, other than limiting or annihilating the decision-making options of a targeted audience.[228] A compelling influence operation does not provide facts and reasons in a neutral way, forcing people to make a choice they would otherwise not make.[229] As there are no 'acceptable alternatives',[230] the opponent is forced to act.

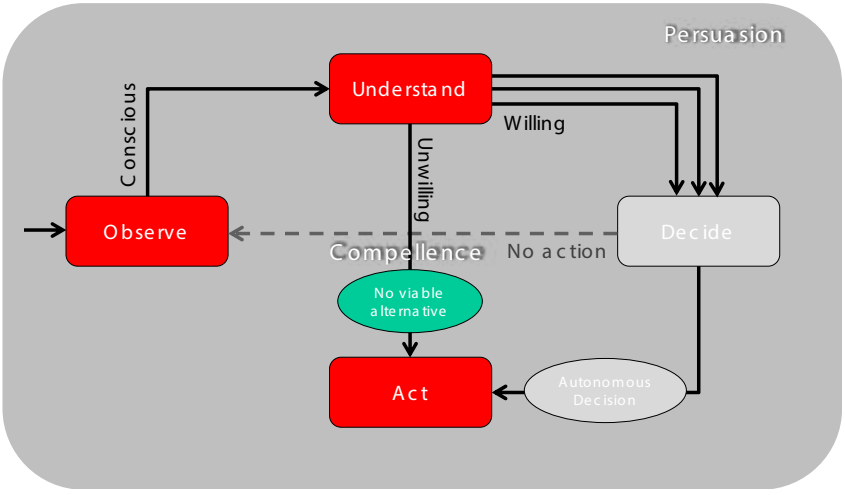

Figure 2 - 8 Conscious Compelling Influence Operations

224 Korteling, Brouwer, and Toet, "A Neural Network Framework for Cognitive Bias." p. 3.

225 Pligt and Vliek, *The Psychology of Influence : Theory, Research and Practice*. p. 42.

226 Kragh and Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case." p. 807.

227 Steven Wheatley, "Regulating the Frontiers of Hybrid-Warfare: The International Law on Foreign State Cyber," in *New Technologies: New Challenges for Democracy and International Law*, 2019, 1–27. p. 4; Steven Wheatley, "Foreign Interference in Elections under the Non-Intervention Principle: We Need to Talk about 'Coercion,'" *Duke Journal of Comparative and International Law* 30, no. 3 (2020). p. 15.

228 Or as Appelbaum states: coercion is "universally recognized as vitiating that person's decision and thus rendering consent invalid". Paul S. Appelbaum, *Informed Consent of Research Subjects*, *International Encyclopedia of the Social & Behavioral Sciences: Second Edition*, Second Edi, vol. 12 (Elsevier, 2015). p. 112.

229 Kilovaty, "Legally Cognizable Manipulation." p. 463; Sunstein, "Fifty Shades of Manipulation." p. 220.

230 Wood, "Coercion, Manipulation, Exploitation." p. 21.

Though both persuasive and compelling influence operations target the cognitive dimension, the persuasive act attempts to change the attitude whilst the compelling act results in a change of behaviour.[231] Compelling influence operations force the targeted audience to eliminate all options except the one aligned with the demands of the compeller.[232]
Reversing this argument, influence operations that limit or short-cut the deliberate understanding and autonomous decision-making are compelling by nature,[233] especially if the alternatives are (or presented as) less favourable.[234]

A targeted audience or person that is being persuaded will keep the possibility of making a free choice while compellence robs them of a choice, but in both cases the 'capacity for conscious decision-making remains intact'.[235] Conversely, manipulation attempts to subvert, undermine and even take control of that capacity of the targeted audience.[236] Manipulation does not aim to influence the belief but uses psychological levers, which are social and cognitive heuristics to achieve biased results, often in a covert manner.[237] Kilovaty argues that manipulation is hidden from the subject of manipulation; it exploits weaknesses of the subject based on available data or algorithms; and it is targeted, meaning that the subject receives bespoke messages in order to facilitate cognitive or behavioural changes.[238] Waltzman coined the phrase 'cognitive hacking' (contrary to ICT hacking), whose core elements of success are the 'unprecedented speed and extent of disinformation distribution, (and the) authors' correct assessment of their intended audiences' cognitive vulnerability—a premise that the audience is already predisposed to accept because it appeals to existing fears or anxieties'.[239] Apart from disinformation, examples of soft-cyber operations are trolling campaigns or the leaking of sensitive information.[240]

231 BJ Fogg, *Persuasive Technology : Using Computers to Change What We Think and Do*, The Morgan Kaufmann Series in Interactive Technologies (Amsterdam: Morgan Kaufmann, 2003). p. 8; Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (2017): 452–81. P. 455; Thomas C Schelling, *Arms and Influence*, *Harvard University. Center for International Affairs*, Affairs., (New Haven SE - viii, 293 pages 23 cm: Yale University Press, 1966). pp. 3-4.

232 Compliance can be achieved by coercion and enticement, is a short-term change in behaviour. Kim Cragin and Scott Gerwehr, *Dissuading Terror Strategic Influence and the Struggle Against Terrorism*, 2005. pp. 15-20.

233 Change behaviour in a compelling way without the use of force is e.g. children's potty training by their parents where the children are forced to change their behaviour without options given.

234 Ohlin, *Election Interference: International Law and the Future of Democracy*. pp. 79-81.

235 Susser, Roessler, and Nissenbaum, "Online Manipulation: Hidden Influences in a Digital World." p. 15.

236 Susser et al. see nudging and deception as subsets of manipulation, see Susser, Roessler, and Nissenbaum. pp. 21- 26.

237 Susser, Roessler, and Nissenbaum. p. 22.

238 Kilovaty, "Legally Cognizable Manipulation." p. 464.

239 Rand Waltzman, "The Weaponization of Information: The Need for Cognitive Security," *Testimony Presented before the Senate Armed Services Committee, Subcommittee on Cybersecurity*, 2017.

240 In a broader setting (not limited to cyberspace) the RF make the division between activities with an informational-technical effect, and those with an informational-psychological effect, attempting to change the belief and behaviour or targeted audiences. See: Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict*. p. 73.

Manipulative influence operations make deliberate use of cognitive heuristic reflexes,[241] and 'take advantage of human cognitive and emotional biases'.[242] These subconscious techniques circumvent, subvert or even usurp[243] the understanding and decision-making process in a way that can be harmful, confusing or disadvantageous to the receiver,[244] and ultimately influence targeted audiences[245] in making quick judgments[246] instead of deliberate appreciations and decisions.[247] Manipulative influence operations are not wrongful per se, not least since these are a common practice in commercials and advertisements. They can be wrongful if they leave the targeted audience no meaningful options to choose from, in which case the manipulative influence operation transgresses into a compelling one.

Cognitive and social heuristics or 'rules of thumb'[248] are psychological reflexes which set in during conditions of time constraints, or while there is shortage or an overload of information.[249] Usually the outcome of these 'mental shortcuts' are 'highly economical and usually effective';[250] however, they can also lead to suboptimal judgments or biases. By using heuristics or mental shortcuts the targeted audiences of State B receive specially-prepared information inclining[251] them to make a voluntarily predetermined choice favouring the priorities of State A. The judgments made[252] may result in behaviour over which the target audience has incomplete, volitional control.[253]

241 Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare." p. 4.

242 Sander, "Democray under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections." p. 11; Lin and Kerr, "On Cyber-Enabled Information / Influence Warfare and Manipulation." pp. 8-9; Hollis, "The Influence of War; The War for Influence." pp. 38-39.

243 Wood, "Coercion, Manipulation, Exploitation." p. 18.

244 Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare." p. 8; Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict*. pp. 13-15.

245 Lin and Kerr, "On Cyber-Enabled Information / Influence Warfare and Manipulation.", pp. 4-5; See also Hollis, "The Influence of War; The War for Influence." p. 38. See also: Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare.", pp. 12-34.

246 Pligt and Vliek, *The Psychology of Influence : Theory, Research and Practice*. p. 59.

247 Similar 'conditioned reflexes' are thought as drill during military basic training, see: Richard Holmes, *Acts of War: The Behavior of Men in Battle*, *Free Press*, 1st US Ed. (New York: Free Press, 1986). p. 39. But most prominently during commercials, advertisements and other expressions of marketing.

248 Daniel Kahneman, "A Perspective on Judgment and Choice: Mapping Bounded Rationality," *American Psychologist* 58, no. 9 (2003): 697–720. p. 711.

249 Kristina Lerman, "Information Is Not a Virus, and Other Consequences of Human Cognitive Limits," *Future Internet* 8, no. 2 (2016): 1–11. p. 8.

250 Tversky and Kahneman, "Judgment under Uncertainty: Heuristics and Biases." p. 1131.

251 A method also use by the Russian concept of 'reflexive control'. Thomas, "Russia's Reflexive Control Theory and the Military." p. 237.

252 Toet et al., "Effects of Personal Characteristics on Susceptibility to Decision Bias : A Literature Study." p. 1.

253 Icek Ajzen, "Theory of Planned Behavior," *Journal of Health Psychology* 12, no. 1 (1991): 1–8. p. 181.

Cognitive heuristics are intuitive short-cuts in our cognitive assessment which, due to distorting principles,[254] could lead to biases in our attitude and behaviour.[255] Though heuristics and biases are numerous, they can be categorised by segments: availability, adjustment and anchoring, and representativeness.[256]

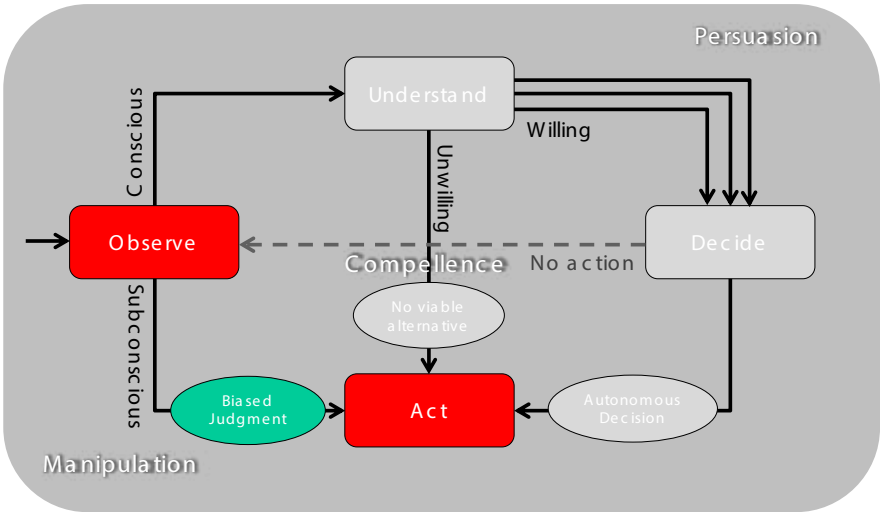

Figure 2 - 9 Subconscious Manipulative Influence Operation

The availability heuristic means that people assess frequency or probability of an event by 'the ease with which an occurrence is brought to mind.'[257] The reason this heuristic sets in is the associative construct of the human neural networks, seeking for relationships or coherence in available information. Biases resulting from the availability heuristic are related to imaginability (it is difficult to assess something that is not stored in our memory) or the illusory correlation;[258] if events co-occur the biased judgment is that they are related.

254 Korteling, Brouwer, and Toet, "A Neural Network Framework for Cognitive Bias." p. 5. These distorting principles are related to our biological neural network alluding to the tendencies to (1) associate (unrelated) information, (2) to give priority to information that is compatible and consistent with our present knowledge, opinions, and expectations, (3) to retain given information that sometimes better could be ignored, and (4) to focus on dominant information while neglecting relevant information that is not directly available or recognized.

255 The cognitive heuristics are based on Tversky and Kahneman, "Judgment under Uncertainty: Heuristics and Biases." and the distorting principles on Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare." pp. 12-30.

256 Different scholars use alternating terms for the heuristics, see also: Barfman and Barfman, *Sway: The Irresistible Pull of Irrational Behaviour.*; Dan Ariely, *Predictably Irrational: The Hidden Forces That Shape Our Decisions*, Revised ed (Harper, 2010).; Paul K Davis et al., "Influencing Adversary States: Quelling Perfect Storms" (Santa Monica, 2021). pp. 21-22.

257 Tversky and Kahneman, "Judgment under Uncertainty: Heuristics and Biases." p. 1127.

258 Blair S. Williams, "Heuristics and Biases in Military Decision Making," *Military Review* Sept-Oct (2010). pp. 62-64.

The illusory correlation is a strong bias and very 'resistant to contradictory data'.[259] The adjustment heuristic is closely related to the anchoring heuristic, but the distorting principles are different. Adjustment means that humans make assessments related to a baseline. When predicting tomorrow's weather, we do not make a rational assessment but look at today's weather. The brain looks for information that is consistent with known, recognised and accepted preconceptions.[260] Gorodnichenko and others found that during the UK EU referendum, pro-leave Twitter-users reacted 'faster and stronger to the messages created by other pro-"leave" users.'[261] Ferguson argues that 'telling people what they want to believe is often the most effective way to gain their favor'. Moreover, the confirmation bias resulting from this heuristic induces dopamine rushes validating the human beliefs and 'thereby becomes an addiction for which the current information environment provides a limitless prescription.'[262] The anchoring heuristic could also result in biases related to compatibility, consistency, or confirmation.[263] But, it is also subject to the retainment principle, meaning that the brain captures irrelevant information since it is associated with, or anchored to, other information. Multiple exposure and repetition of information, or disinformation make use of this heuristic. Though the information is misleading or ambiguous to the audiences, long-term and persistent exposure to that information generates cognitive reluctance to change the first imprints.[264] The distorting principle related to this heuristic is availability but also the focus-principle alluding to the tendency to only absorb the dominant information – the known knows.[265] A related bias is stereotyping. In other words, we give value to information with a certain authority, while we ignore or are insensible to other data that could refute existing knowledge.[266]

The social heuristics are authority, likeability, reciprocity, consistency and scarcity.[267] Authority means people comply with legitimate authoritative figures. Likeability refers to the notion that we are more easily persuaded by people we like or groups we feel associated with. Reciprocity means that one feels obliged to repay if something is given.[268] Furthermore,

259 Which relates directly to the illusion of predictable behaviour alluded in § 2.2.3.3. See also: Tversky and Kahneman, "Judgment under Uncertainty: Heuristics and Biases." p. 1128.

260 Ball, *Post-Truth: How Bullshit Conquered the World*. pp. 8-9. Ball called this the 'filter bubble'.

261 Yuriy Gorodnichenko, Tho Pham, and Oleksandr Talavera, "Social Media, Sentiment and Public Opinions: Evidence From #Brexit and #Uselection," *National Bureau of Economic Research*, 2018. p. 23.

262 Michael P. Ferguson, "The Evolution of Disinformation : How Public Opinion Became Proxy," *Strategic Bridge*, 2020.

263 DeMarzo et al. refer to this as the persuasion bias, DeMarzo, Vayanos, and Zwiebel, "Persuasion Bias, Social Influence, and Unidimensional Opinions." pp. 909-913; Fabiana Zollo et al., "Emotional Dynamics in the Age of Misinformation," *PLoS ONE* 10, no. 9 (2015): 1–21. p. 2; The Barfmans call this the 'lure of a diagnosis bias', Barfman and Barfman, *Sway: The Irresistible Pull of Irrational Behaviour*. p. 91.

264 Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare." p. 22.

265 Korteling, Brouwer, and Toet, "A Neural Network Framework for Cognitive Bias." pp. 7-12.

266 Barfman and Barfman, *Sway: The Irresistible Pull of Irrational Behaviour*. pp. 48-49; Tversky and Kahneman, "Judgment under Uncertainty: Heuristics and Biases." pp. 1124-1125.

267 Cialdini, *Influence: The Psychology of Persuasion*. p. ix.

268 Cialdini. p. 17.

consistency means that people prefer that others 'practise what they preach' and are averse to hypocrisy. Finally, the scarcity heuristics indicates that if something is seemingly scarce, we have the urge to desire it.[269]

Russian 'Active Measures' rely on the heuristics in what is called reflexive control[270] i.e. 'conveying to a partner or an opponent specially-prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action.'[271] The Active Measures-doctrine was developed in the interbellum and seeks to find strategic advantages in the information environment by deception, forgeries,[272] provocation, subversion,[273] but also by the spreading of disinformation.[274] With this mechanism Russia seeks to influence the target audience in a subconscious manner utilising the cognitive biases i.e. the limitations in the available data and in the human information processing capacity.[275]

Induced by lies, false, fabricated, doctored and deceitful information, manipulative influence operations making use of subconscious techniques which invoke cognitive and social heuristics can be compelling in nature as these operations aim to undermine the target's ability to make meaningful decisions. Not least because the target can no longer rely on its own perceptions, memories, beliefs or moral judgment, or will not have the ability to assess the authenticity of the source (outlet) of information. Wood states that in certain circumstances manipulative influence operations making use of lying are the functional equivalent of compellence.[276]

Subconscious manipulation, which is compelling in nature, differs from conscious compellence, since the latter means that the targeted audience is aware of the compelling act and 'bluntly' realises that its options are limited and the alternative is even less preferable, as is the case in an armed robbery. Ohlin, therefore, argues that a manipulative influence operation cannot be compelling, since the element of an undesirable alternative when

269 What Ariely calls the fallacy of demand and supply, see: Ariely, *Predictably Irrational: The Hidden Forces That Shape Our Decisions*. pp. 25 ff.

270 Thomas, "Russia's Reflexive Control Theory and the Military." pp. 238-243.

271 Thomas. p. 237. See also: Ajir and Vailliant, "Russian Information Warfare : Implications for Deterrence Theory." pp. 72-73; Giles, "Handbook of Russian Information Warfare." p. 19.

272 Kragh and Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case."pp. 790-797.

273 Radin, Demus, and Marcinek, "Understanding Russian Subversion: Patterns, Threats, and Responses." pp. 2-3.

274 United States Senate Committee on Intelligence, "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election - Volume 2: Russia's Use of Social Media," vol. 2, 2019. pp. 12-13; EU vs Disinformation, "Election Meddling and Pro-Kremlin Disinformation: What You Need to Know." p. 4; Aceves, "Virtual Hatred: How Russia Tried to Start a Race War in the United States." pp. 185-189.

275 Korteling, Brouwer, and Toet, "A Neural Network Framework for Cognitive Bias." p. 2.

276 Wood, "Coercion, Manipulation, Exploitation." p. 35.

not complying is lacking during manipulation.[277] Others argue that manipulation can transgress into compellence. Wheatley, on the other hand, argues that compellence not only has a physical but also a psychological guise which diminishes options without the targeted audience' awareness. The agent that compels will withhold or selectively feed information creating the suggestion that there is only one sensible choice.[278] This notion of psychological compellence is aligned with manipulation. Wood argues that manipulation is 'usurping someone's free agency'[279], influencing the targeted audiences in a way beneficial to the manipulator. Susser et al. echo this rationale and refer to 'taking hold of the controls' of the targeted audience and 'displacing' them as the decider.[280] Manipulation is dissimilar from physical compellence in that the targeted audience does not consciously make an unwilling choice. However, it is similar with compellence in that it leaves the targeted audience no viable options and circumvents the target audience's deliberate understanding and autonomous decision-making.

In this thesis, compellence will be described in terms of purposeful circumvention of autonomous decision-making and cutting short the deliberate understanding. Influence operations can make use of overt, conscious forms of compellence. Manipulative influence operations making use of subconscious techniques, in which the targeted audience is often unaware of the influence effort, are not compelling per se. However, if the manipulative operations undermine the targeted audiences' understanding and decision-making process in a psychological manner[281] leaving them no meaningful options to choose from, the manipulative influence operation is compelling in nature.

2.2.4.4. Framing

The aim of influence operations is to change the deliberate understanding and autonomous decision-making of State B in a way favourable to State A. Nevertheless, influence operations will only be effective if the audiences of State B are susceptible to the content of the operations. Selecting an objective (intent) and an instrument of power (strategic narrative) will not suffice; in order to be effective, influence operations will need to 'frame' or operationalise the strategic narrative. Depending on the manner of influence – persuasive, compelling or manipulative – State A will frame the strategic narrative making use of conscious and subconscious techniques to influence the targeted audience.[282]

277 Ohlin, *Election Interference: International Law and the Future of Democracy*. pp. 84-85.

278 Wheatley, "Regulating the Frontiers of Hybrid-Warfare: The International Law on Foreign State Cyber." p. 16.

279 Wood, "Coercion, Manipulation, Exploitation." p. 31.

280 Susser, Roessler, and Nissenbaum, "Online Manipulation: Hidden Influences in a Digital World." p. 16.

281 Wheatley, "Foreign Interference in Elections under the Non-Intervention Principle: We Need to Talk about 'Coercion.'" p. 16.

282 Dennis Chong and James N. Druckman, "Framing Public Opinion in Competitive Democracies," *The American Political Science Review* 101, no. 4 (2007): 637–55. p. 639.

Strategic narratives do not automatically influence a targeted audience. To effectuate a narrative it will need to be broken down into simpler structures, a script or a reference frame,[283] which is a specific manner of presenting an issue.[284] The frames of reference are models of understanding in the interaction between specific audiences and texts, images or memes. It examines 'the ways in which narrative texts gratify, frustrate, or in other ways play with these cognitive structures by which we make sense of our world.'[285]

The content or form of strategic messaging needs to be shaped in such a way that it connects with contentions societal topics, and fits with the preference and heuristics of the targeted audience in order to make them receptive to the frame and the narrative. In that sense, Entman defines to frame as 'to select some aspects of perceived reality and make them more salient in a communicating text, in such a way as to promote a particular problem definition, causal interpretation, moral evaluation (…)'.[286]

Frames can affect the attitudes and behaviours of targeted audiences if they emphasize 'available and applicable considerations'.[287] This means that the target audience must be aware of a the salience of a specific event or issue[288] representing a situational or objective element which must be available to them;[289] and the frame must invoke a specific attitude, belief or opinion of a group, which is more subjective.[290] Moreover, the 'magnitude of framing effects depends not only on the strength of the frame but also on the context in which it is presented and the characteristics of the recipient of the frame.'[291]

Framing is the operationalisation of a strategic narrative and when supporting a manipulative influence operations it aims to create a script inclined to let audiences make predetermined (reflexive) judgments based on their biases, aligned with the preferences of the State executing the influence operation, namely State A.[292] As depicted in figure 2.10,

283 Lakoff, *The Political Mind: A Cognitive Scientist's Guide to Your Brain and Its Politics*. pp. 22 ff.

284 Atikcan, Nadeau, and Belnager, *Framing Risky Choices: Brexit and the Dynamics of High-Stakes Referendums*. p. 4.

285 Abbott, *The Cambridge Introduction to Narrative*. p. 30.

286 Robert M Entman, "Framing: Toward Clarification of a Fractured Paradigm," *Journal of Communication* 43, no. 4 (December 1, 1993): 51–58. p. 52.

287 Chong and Druckman, "Framing Public Opinion in Competitive Democracies." pp. 639-640.

288 Entman, "Framing: Toward Clarification of a Fractured Paradigm." p. 53.

289 Atikcan et al. argue that frames have three psychological effects: availability, accessibility and applicability. Frames must address existing beliefs, voters should be able to comprehend them, and applicable to their situation. Frames from credible sources and related to specific values enjoy higher applicability and strength. Atikcan, Nadeau, and Belnager, *Framing Risky Choices: Brexit and the Dynamics of High-Stakes Referendums*. p. 16.

290 Chong and Druckman, "Framing Theory." pp. 106-109.

291 Chong and Druckman, "Framing Public Opinion in Competitive Democracies." p. 640.

292 A narrative can have several frames, or 'influence efforts'. Diego A. Martin and Jacob N. Shapiro, "Trends in Online Foreign Influence Efforts," *ESOC Publications*, 2019. p. 4.

framing couples the narrative, socially divisive topics and reflexive preferences or heuristics of groups to an event.[293]

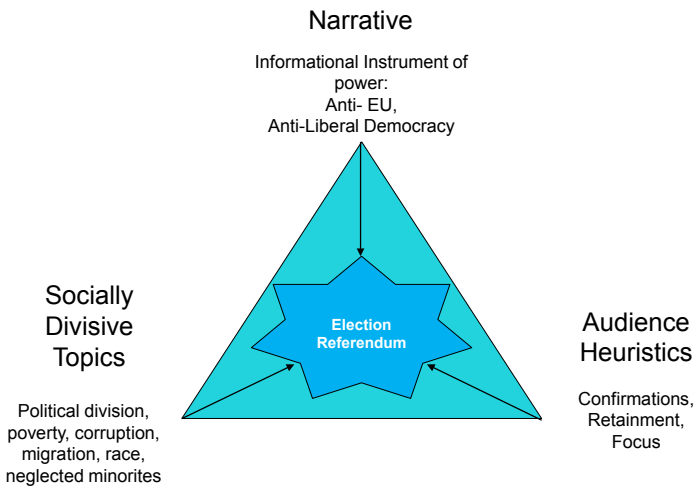

Figure 2 - 10 Framing the Narrative

Events to be utilised for a frame can be a scheduled or ad-hoc foreign or domestic event, such as an election, a demonstration, referendum or pandemic, such as Covid-19.[294] To illustrate this, during the UK EU referendum, the Vote Leave camp coined the frame: 'let's take back control'.[295] This frame made the connection between the available societal topics (related to economic malaise and immigration) and applicable considerations for a specific audience on the basis of their feeling (related to the heuristics) that the UK is not allowed to make sovereign choices. The available and accessible considerations were linked to the EU and to the possibility of making a change via the context of the EU referendum. It is not necessary that these items are connected in reality, nor that the correlation made is true, but they must

293 Pijpers and Ducheine, "Influence Operations in Cyberspace - How They Really Work." pp. 11-15.

294 See e.g. Rachel Brown, Heather Hurlburt, and Alexandra Stark, "How the Coronavirus Sows Civil Conflict," Foreign Affairs, 2020, https://www.foreignaffairs.com/articles/world/2020-06-06/how-coronavirus-sows-civil-conflict.

295 Atikcan, Nadeau, and Belnager, *Framing Risky Choices: Brexit and the Dynamics of High-Stakes Referendums*. p. 5; Dominic Cummings, "How the Brexit Referendum Was Won," *The Spectator*, 2017.

appear to be true or realistic, appeal to the targeted audience,[296] resonate with existing concerns,[297] and be 'indigenous to the target State'.[298]

Socially divisive topics are addressed using the communication dynamics of societies,[299] i.e. the tendency to commence a discourse on topics on which various opinions exist in a society e.g. combatting poverty, racism, tax evasion, language feuds. Addressing socially divisive topics can be inducive to sow discord in a society or any other targeted audience (e.g. the diaspora of State B in State A) or even generate polarisation.[300] Scripting and framing efforts can make use of differences between groups,[301] accentuate feelings of rejection and neglect with minority groups, fuel internal divisions over political issues such as poverty, migration, rights of minorities or LGBT, and allegations of corruption and inefficiency of established institutions.[302] During the UK EU referendum in 2016, the Vote Leave camp made the suggestion that the period of societal mishaps concerning immigration, unemployment or lack of economic progress coalesced with the period of UK membership to the EU implying a link between the two and using the EU as a scapegoat.[303]

Clearly defining socially divisive topics requires research and the collection of data to gain understanding of the strengths and weaknesses of a society and its targeted audience.[304] Furthermore, data of the demography of the target audiences are required concerning age, gender, education, finance, location,[305] but also about the language used in the discussions and the platforms of discussion. The more refined and elaborate the data, the more effective the influence operation: it may be argued that the failure of the influence operations during the 2017 French elections (allegedly by RF and American (US) alt-right activists) was partly due to lack of knowledge of the French language and culture.[306]

Socially divisive topics add realism to the frame which addresses the conscious part of cognition, such as in the frame used during the UK EU referendum regarding the UK weekly contribution of £350m per week to the EU which could also be used to strengthen the

296 Atikcan, Nadeau, and Belnager, *Framing Risky Choices: Brexit and the Dynamics of High-Stakes Referendums*. p. 18.

297 Atikcan, Nadeau, and Belnager. p. 4.

298 Martin and Shapiro, "Trends in Online Foreign Influence Efforts." p. 4.

299 Tansino, "Analysing Strategic Communications through Early Modern Theatre." p. 55.

300 Cleavages in society are i.a. ethnicity, class and religion, see: Lane and Ersson, *Politics and Society in Western Europe*. pp. 44 ff.

301 Larson et al., *Foundations of Effective Influence Operations*. pp. 75-77.

302 Jeangene Vilmer, "Information Manipulation: A Challenge for Our Democracies." pp. 65-70.

303 Atikcan, Nadeau, and Belnager, *Framing Risky Choices: Brexit and the Dynamics of High-Stakes Referendums*. pp. 95 ff.

304 Filipe N. Ribeiro et al., "On Microtargeting Socially Divisive Ads: A Case Study of Russia-Linked Ad Campaigns on Facebook," *FAT* 2019 - Proceedings of the 2019 Conference on Fairness, Accountability, and Transparency*, 2019, 140–49.; Larson et al., *Foundations of Effective Influence Operations*. pp. 114-116.

305 Information Commissioner's Office, "Democracy Disrupted? Personal Information and Political Influence," 2018. p. 22.

306 Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." p. 28; See also infra Chapter 4.4.

National Health Service (NHS).[307] A frame could be further strengthened by pointing to a – less favourable – alternatives if the preferred avenue (or voting advice) is not followed,[308] as depicted in the NHS-frame but also in the Vote Leave-frame of 'taking back control'.
But frames can also benefit from cognitive and social heuristics i.e. the concept that human thinking is guided by unconscious mental structures'[309] or reflexive responses triggered by specific words or images. Frames intentionally target the subconscious cognitive process of a group to affect their beliefs and behaviour,[310] and thus the sentiment of the target audiences.[311]

Therefore, during the preparation of influence operations, socially divisive topics and audiences in a certain society, need to be connected to heuristics that trigger the ideology, preferences or (pre)judgments of specific audiences in that society. Knowledge of preferences or biases of the audiences and target groups must be 'harvested' based on political preferences, ethnical background, affiliations (i.e. membership of the National Rifle Association in the US), voting behaviour, on-line consumer and social behaviour, mode of transport and so on.[312] Relevant elements of framing are the use of words or metaphors (e.g. Pro-Life, Axis of Evil, War on Terror) which activate heuristics such as the retainment and the compatibility principles.[313] The more granular the data related to the audience, the more effective the content of a soft-cyber operation will be, as was illustrated by activities supported by the data-mining firm Cambridge Analytica.[314]

The so-called Lisa Case[315] was an example of the use a framed disinformation campaign in which fictitious causality was applied.[316] During this incident in Germany, a girl of Russian descent was lost for a few hours. The Russian media had picked up this topic and suggested that

307 "What Would Happen ... If We Vote to Leave the EU," voteleavetakecontrol.org, 2016, http://www.voteleavetakecontrol.org/why_vote_leave.html.

308 Chong and Druckman, "Framing Public Opinion in Competitive Democracies." p. 638.

309 Gorton, "Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy." p. 62.

310 Martin & Shapiro use on-line influence effort to state the same. Martin and Shapiro, "Trends in Online Foreign Influence Efforts." P.4; Gorton, "Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy." p. 75.

311 EU vs Disinformation, "Election Meddling and Pro-Kremlin Disinformation: What You Need to Know." p. 3.

312 The bias scores on Facebook is a well-known tool ('thisisyourdigitallife' or 'My Personality') to gather these data. Cambridge Analytica claimed to have thousands of attributes of a large segment of American voters (50-87 Million) See also: Information Commissioner's Office, "Investigation into the Use of Data Analytics in Political Campaigns." pp. 16-18; Susser, Roessler, and Nissenbaum, "Online Manipulation: Hidden Influences in a Digital World." p. 10; Kilovaty, "Legally Cognizable Manipulation." pp. 466-467; Cambridge Analytica, "CA Political: An Overview of Cambridge Analytica's Political Division," 2016. (available at https://ia803204.us.archive.org/35/items/ca-docs-with-redactions-sept-23-2020-4pm/FINAL%20Cambridge%20Analytica%20Select%202016%20Campaign%20Related%20Documents%20w%20Redactions_.pdf)

313 Lakoff, *The Political Mind: A Cognitive Scientist's Guide to Your Brain and Its Politics*. pp. 22 ff.

314 Roberto J. González, "Hacking the Citizenry?: Personality Profiling, 'Big Data' and the Election of Donald Trump," *Anthropology Today* 33, no. 3 (2017): 9–12. p. 9.

315 Mahairas and Dvilyanski, "Disinformation – (Dezinformatsiya)." pp. 23-26.

316 Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare." pp. 13-14.

Lisa was abducted and raped by an 'Arab'-looking person.[317] The RF's aim is to create strategic confusion accompanied by an anti-EU and anti-liberal democracy- narrative. This incident was seized on and attached to socially divisive topics regarding migration (for the German audience) and the protection of Russian minorities abroad (for the domestic audience). The event was further coupled to existing views, stereotypes and pre-judgments within societies about North-African or Arab people. To some groups the story was a confirmation of their views, and more neutral people could not ignore yet another topic focusing on issues with migrants or Arab people. It also anchored the perception that these foreigners (when in a host country) have bad intentions. It came out that the story was entirely made up and there was neither connection nor causality whatsoever between the elements of the story. Nevertheless, it gave rise to discussions on migrants in Germany and on the German position within the EU on that topic, apart from causing a major row with Russia.[318]

Frames that include subconscious elements are an essential part of the RF concept of 'reflexive control',[319] which can be defined as a 'conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action.'[320] The reflexive control-doctrine seeks to influence the audience in a subconscious manner utilising the invocation of cognitive biases based on the limitation of human information processing capacities.[321] Subconscious influence operations, on which the RF reflexive control is also based, rely on the tendencies to associate seemingly unrelated data, as was the situation in the Lisa Case. Via a process of anchoring, stereotyping and applying spurious causality, a migrant was associated with the alleged disappearance of a girl.[322] Subconscious influence operations also use heuristics that tempt us to remember or retain information which is not relevant[323] and give priority to information that is compatible and consistent with existing knowledge, opinions, and preferences,[324] and which focuses on dominant and easily accessible information. As such, a

317 Mahairas and Dvilyanski, "Disinformation – (Dezinformatsiya)." p. 23.

318 Jakub Janda, "The Lisa Case: STRATCOM Lessons for European States," *Federal Academy for Security Policy*, no. 11 (2016): 1–4.

319 Thomas, "Russia's Reflexive Control Theory and the Military." pp. 238-243; Kilovaty, "Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information." pp. 158-160.

320 Thomas, "Russia's Reflexive Control Theory and the Military." p. 237. See also: Ajir and Vailliant, "Russian Information Warfare : Implications for Deterrence Theory." pp. 72-73; Giles, "Handbook of Russian Information Warfare." p. 19.

321 Ribeiro et al., "On Microtargeting Socially Divisive Ads: A Case Study of Russia-Linked Ad Campaigns on Facebook." pp. 147-148; Korteling, Brouwer, and Toet, "A Neural Network Framework for Cognitive Bias." p. 2.

322 Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare." pp. 13-14.

323 To illustrate how the mind works, George Lakoff often starts lectures on cognitive science with the phrase: 'don't think about the elephant' which can't be done as it evokes an image that is difficult to negate. George Lakoff, *Don't Think of an Elephant: Know Your Values and Frame the Debate*, *Chelsea Green Publishers*, 2004.; George Lakoff, "Framing the Dems: How Conservatives Control Political Debate and How Progressives Can Take It Back," *The American Prospect*, 2003. p. 32; Lakoff, *The Political Mind: A Cognitive Scientist's Guide to Your Brain and Its Politics*. pp. 232- 233.

324 Korteling, Brouwer, and Toet, "A Neural Network Framework for Cognitive Bias." p. 5; Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare." pp. 15-19.

Twitter account with many followers or 'likes' is 'dominant' over accounts with fewer 'likes', irrespective of the authenticity of the content.

Frames create templates in which all further activities, content and communications can be embedded,[325] similar to what the Russian Active Measures-doctrine says.[326] Active Measures are particularly adept in utilising socially divisive topics or as Rid remarked: "The tried and tested way of active measures is to use an adversary's existing weaknesses against himself, to drive wedges into pre-existing cracks: the more polarized a society, the more vulnerable it is."[327]

The emergence of cyberspace did not only invigorate the RF's Active Measures, but the characteristics of cyberspace have made it possible to use cognitive and social heuristics as an instrument in generating (the illusion) of predictable or planned behaviour.[328]
Cognitive and social heuristics are difficult to use as instruments to influence targeted audiences since these neural, emotional and psychological reflexes cannot be accessed directly and may differ per group. The reflexes can be approximated by making use of 'computational' social sciences. By analysing large data sets based on social media profiles, correlations can be extracted and used to trigger the invocation of social or cognitive heuristics, including via 'computational propaganda'.[329]

Framing applies both conscious and subconscious techniques to make audiences receptive for a narrative. The conscious elements, including socially divisive topics, are required to generate an air of realism to the frame, whereas subconscious heuristics and biases are needed to create reflexive responses. Frames based on consciously construed socially divisive topics are more persuasive in nature. However, the more frames for influence operations rely on social and cognitive subconscious heuristics, the more manipulative they are since they will shortcut or bypass deliberate understanding and autonomous decision-making, inclining a biased judgment.

325 In the Ukrainian- RF conflict, the RF narrative is that this is an internal conflict, not an inter-State conflict. Hence the RF will regard intervention by the UN Security Council, that is not authorised to intervene in internal conflicts, as inappropriate.

326 Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (London: Profile Books, 2020). pp 6-14; Giles, "Handbook of Russian Information Warfare." pp. 19-21, though the latter terms are, like hybrid warfare, Western connotations not used in the Slavic tongue.

327 Thomas Rid, "Disinformation: A Primer in Russian Active Measures and Influence Campaigns," *Select Committee on Intelligence United States Senate*, (2017). p. 2.

328 Icek Ajzen, "The Theory of Planned Behaviour: Reactions and Reflections," *Psychology and Health* 26, no. 9 (2011): 1113–27.; Kosinski, Stillwell, and Graepel, "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior."

329 Philip N. Howard and Bence Kollanyi, "Bots, # StrongerIn, and # Brexit: Computational Propaganda during the UK-EU Referendum," *Comprop Research Note 2016.1*, 2016.; Woolley and Howard, "Political Communication, Computational Propaganda, and Autonomous Agents: Introduction."

2.2.5. Cyber-related activities to change behaviour and attitude

Preparing influence operations require formulating political intent, the choice of an instrument of power (strategic narrative), and the operationalisation of the narrative in one or several frames. The frames use conscious and subconscious techniques giving them a persuasive, compelling or manipulative character.

Influence operations are executed via the use of cyber-related activities including disinformation,[330] trolling, leaking of private information,[331] and political grooming campaigns,[332] with the aim to surgically influence the understanding and decision-making process.[333] The cyber-related activities are used to target the audiences and generate the effects of changing the behaviour and attitude of the targeted State (see figure 2.11). These activities are not mutually exclusive and far from new.[334] When executed in cyberspace, influence activities such as disinformation or leaking of sensitive data, are deliberate soft-cyber activities that fit within a larger plan (the strategic narrative), and are preferably synchronised in time and aligned with (or in support of) other physical activities,[335] including hard-cyber operations that target the logical layer, disrupt or manipulate the cyber infrastructure such as electronic voting machines or vote counts.[336]

330 E.g. 2014 Ukrainian elections; 2016 Dutch referendum on the EU-Ukraine Association Agreement; 2016 Brexit referendum; 2016 US elections; 2017 Catalan independence referendum; 2017 German elections; 2017 French elections; 2018 Italian elections. EU vs Disinformation, "Election Meddling and Pro-Kremlin Disinformation: What You Need to Know." p. 2.

331 Chris Tenove et al., *Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy*, *Centre for the Study of Democratic Institutions* (University of British Colombia, 2018). pp. 16-23; Barrie Sander, "The Sound of Silence : International Law and the Governance of Peacetime Cyber Operations," 2019, 1–21. p. 16.

332 Alina Polyakova and Spencer P Boyer, "The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition the New Geopolitics," *Brookings - Robert Bosch Foundation*, no. March (2018). p. 8.

333 Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare." pp. 4-5. Korteling et al. describes that "human reasoning and decision-making show systematic simplifications or 'mental shortcuts' to speed up the decision-making process. These shortcuts are commonly known as 'heuristics' and may often produce acceptable outcomes. However, these intuitive distortions also tend to violate the rules of logic and probability, which even so often lead to suboptimal judgments and decisions, called biases".

334 Constance Holden, "Curbing Soviet Disinformation," *Science* 242, no. 4879 (1988). p. 665, related to alleged disinformation on AIDS; Nicholas J. Cull et al., "Soviet Subversion, Disinformation and Propaganda: How the West Fought Against It: An Analytic History, with Lessons for the Present," 2017. pp. 1-6.

335 E.g. during the RF annexation of the Crimea, see: Bouwmeester, *Krym Nash: An Analysis of Modern Russian Deception Warfare*. sections 8.4 and 8.5.

336 Polyakova and Boyer, "The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition the New Geopolitics." p. 9. Note that influence operations often are part of a coordinated effort which could include all instruments of power effective in all domains.

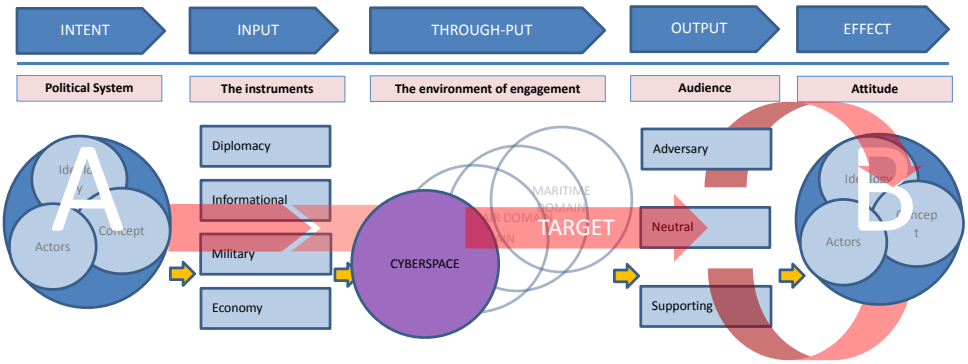

Figure 2 - 11 Generating effects

The frames, operationalising the strategic narrative, will serve as a template for applying and executing the cyber-related activities regarding disinformation, trolling, leaking of sensitive information, and political grooming.[337] The cyber-related activities implement the frames using both the content and the source (outlet) of the message as an instrument.[338] It is not only the content that can be harmful, but also spreading messages (factual or fabricated) with the wrong context or from an unexpected media outlet can cause confusion.[339]

2.2.5.1. *Disinformation*

Disinformation is not merely fake news, a populist 'white lie' or spontaneous political rhetoric.[340] Disinformation[341] is the deliberate spreading of carefully constructed and

337 Tenove et al, and Martin & Shapiro make a similar categorisation for digital interference in elections. Tenove et al incorporating the hard-cyber hacks. See: Tenove et al., *Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy*. pp. 12-25. While Martin & Shapiro make a distinction between defamation, persuasion and polarisation. See: Martin and Shapiro, "Trends in Online Foreign Influence Efforts." p. 8; Hansen and Lim make a distinction between doxing (hack and leak), disinformation, and trolling. See: Isabella Hansen and Darren J. Lim, "Doxing Democracy: Influencing Elections via Cyber Voter Interference," *Contemporary Politics* 25, no. 2 (2019): 150–71. p. 157.

338 Including extreme examples such as Deepfakes, see: Keir Giles, Kim Hartmann, and Munira Mustaffa, "The Role of Deepfakes in Malign Influence Campaigns," *NATO Strategic Communication Centre of Exellence*, 2019. pp. 8-11.

339 Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law." p. 191.

340 The term 'fake news' will therefore not be used as concept in this research, see also: Rid, *Active Measures: The Secret History of Disinformation and Political Warfare*. pp. 9-10.

341 Alexander Lanoszka, "Disinformation in International Politics," *European Journal of International Security*, no. 4 (2019): 227–48. p. 229; House of Commons Digital Culture Media and Sport Committee, "Disinformation and ' Fake News ': Interim Report," 2018. pp. 7-8.

verifiably false[342] or falsified[343] and misleading information,[344] in order to deceive decision-making.[345] Disinformation is created, presented and disseminated for economic gain or ideological purposes,[346] to intentionally deceive the public or a specific audience and may cause public harm including threats to democratic political and policy-making processes[347] by sowing discord among targeted audiences,[348] as illustrated in the above Lisa Case.

The disinformation campaign will amplify social division by disseminating misleading, false, and divisive content. But also by leaving essential data out of a newsflash, concealing the true relation between two facts, or creating new relations, hiding valuable information in an overwhelming mass of disseminated data, oversimplifying events, repeating messages, concealing the source of the data, or changing a (national) position occasionally.[349] Disinformation makes use of perceptions and beliefs that are regarded as controversial.[350] Misleading an audience by disseminating factual news via an unexpected or dubious outlet would also count as disinformation.[351] Mimicking or pretending to be someone else or using so-called sock puppets could be deceptive for the receiving audiences.[352]

Disinformation is subtle in nature and the frame it is based upon applies to both the conscious and subconscious influence techniques of the frame. The conscious element relates to socially divisive topics and provides a sense of realism, while the subconscious part uses heuristics, among others related to the anchoring, confirmation and retainment principle, which means that, once perceived and digested, information is 'trapped'.[353] In cyberspace the 'trapped' fabricated news can benefit from continued and consistent repetition of the

342 Allcott and Gentzkow, "Social Media and Fake News in the 2016 Election." p. 213.

343 Jeangene Vilmer, "Information Manipulation: A Challenge for Our Democracies." p. 88.

344 This includes masquerading the true source of disclosure. See also: Ohlin, *Election Interference: International Law and the Future of Democracy*. p. 17.

345 Kragh and Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case." p. 778.

346 Allcott speaks, in other words, about pecuniary or ideological motivation. Allcott and Gentzkow, "Social Media and Fake News in the 2016 Election." p. 217.

347 Sander, "Democray under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections." p. 11.; Rid, *Active Measures: The Secret History of Disinformation and Political Warfare*. p. 10; Sander, "The Sound of Silence : International Law and the Governance of Peacetime Cyber Operations." p. 16. See also: the House of Commons: Digital, Culture, Media and Sport Committee, Disinformation and 'fake news': Interim Report, 2018 bullet 160.

348 Mahairas and Dvilyanski, "Disinformation – (Dezinformatsiya)." p. 21.

349 Thomas, "Russia's Reflexive Control Theory and the Military." p. 245.

350 Garth S. Jowett, "Propaganda and Communication: The Re-Emergence of a Research Tradition," *Journal of Communication* Winter, no. 37 (1987). p. 101.

351 Yablokov argues that media outlet such as RT is also a 'source of news neglected by the global media juggernauts, such as CNN or BBC World News'. Yablokov, "Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of Russia Today (RT)." p. 301.

352 Savvas Zannettou et al., "Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and Their Influence on the Web," *Arxiv*, 2019. p. 9.

353 Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare." p. 19. As in the famous example 'do not think about the pink elephant'.

message, for instance with Twitter-bots,[354] making use of the compatibility principle,[355] as will be further explained in the section on exploiting social media below.

Invoking subconscious heuristics related to disinformation relies on the inability to give meaning to the data provided but also on the burden of memory or ingrained knowledge. When disinformation is shared or broadcast at the right moment, it also makes use of the focus principle. The 'focus principle' highlights that humans focus on the information that is available or pops up in our minds when having a discussion or making a decision. Information that is just out of our reach is discarded, our so-called blind spot. Disinformation can also make use of the associative principle when using credible persons or outlets to disseminate the data. Astroturfing, or State or commercial cyber initiatives disguised as grassroots activism, makes use of these persuasive and deceptive heuristics.[356] To be susceptive, the frame governing the disinformation campaign must 'at least partially respond to reality, or at least to accepted views'.[357] In the run-up to the 2016 UK EU referendum, the Vote Leave camp sent numerous feeds via social media platforms which lured specific audiences to the Vote Leave sites. These messages were related to football or endangered species such as the polar bear. When clicking on certain buttons a message popped up explaining what the EU was planning to do with football or the polar bear, hence dissuading audiences from voting in favour of staying 'in'.

Disinformation activities are also part of the RF Active Measures, and these cyber-related activities are used to undermine and counter the Western political narrative and trans-Atlantic institutions, but also to sow discord and to paralyse the democratic process,[358] with the intent to blur the line between fact and fiction.[359]

2.2.5.2. *Trolling*

Spreading mal-information – or trolling – is the deliberate act of making discriminatory, abusive or otherwise controversial remarks on the Internet with the aim to harm other

354 Gorodnichenko, Pham, and Talavera, "Social Media, Sentiment and Public Opinions: Evidence From #Brexit and #Uselection." p. 22.

355 Korteling, Brouwer, and Toet, "A Neural Network Framework for Cognitive Bias." p. 8.

356 Mark Leiser, "AstroTurfing, 'CyberTurfing' and Other Online Persuasion Campaigns," *European Journal of Law and Technology* 7, no. 1 (2016): 1–27. p. 5.

357 Rid, *Active Measures: The Secret History of Disinformation and Political Warfare*. pp. 4-5. Rid quotes Ladislav Bittman who he had interviewed.

358 Aceves, "Virtual Hatred: How Russia Tried to Start a Race War in the United States." p. 192.

359 Richey, "Contemporary Russian Revisionism: Understanding the Kremlin's Hybrid Warfare and the Strategic and Tactical Deployment of Disinformation." p. 109; Baezner and Robin, "Cyber and Information Warfare in Elections in Europe." p. 9; EU vs Disinformation, "Election Meddling and Pro-Kremlin Disinformation: What You Need to Know." p. 2; Polyakova and Boyer, "The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition the New Geopolitics." pp. 4-5.

persons,[360] organisations or States.[361] The content of trolling campaigns fuels extreme ideologies, hyper partisanship, or conspiratorial political ideas in order to polarise audiences.[362] The aim is to strengthen the shared visions within (already polarised) groups, and to align the attitude of a group despite heterogeneous or diverging ideas, including absorbing changes in external circumstances. During the 2016 US presidential elections, the Russian 'Internet Research Agency (IRA)'[363] launched numerous social media campaigns that resulted, not only in sowing discord but also in polarisation. Polarisation means strengthening the perceptions of already highly divided audiences,[364] utilising 'echo chambers'[365] or 'filter bubbles'[366] available via social media.[367]

The content is deliberately doctored, seeking to target and ridicule moral virtues or failings of organisations, causes or people. Where disinformation has more in common with classical propaganda, political trolling injects cynicism into the content stimulating disengagement. While disinformation aims to sow discord and confusion, the result of mal-information is to increase in-group identification and hence the difference between groups in a community or society.[368] State-sponsored trolling can lead to intimidation, self-censorship and silencing among dissenting actors in a State.[369]

RF influence operations use trolling activities in order to highlight specific societal issues or dissuade specific groups from casting their vote. In recent years activities of the IRA

360 Alexandra Deem and Laura Csuka, "Hate Speech, Information Disorder, and Conflict," 2020. p. 4.

361 Sander, "The Sound of Silence : International Law and the Governance of Peacetime Cyber Operations." p. 16. In some policy and academic literature trolling is seen as a species of disinformation, a rationale that will not be followed due to the deliberate abusive nature of trolling. See also: United States Senate Committee on Intelligence, "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election - Volume 2: Russia's Use of Social Media." p. 18.

362 Martin and Shapiro, "Trends in Online Foreign Influence Efforts." p. 8.

363 The IRA is a RF agency known for spreading disinformation and mal-information, therefore also known as the troll-factory. Though the IRA is not a government agency as such it does have close ties with the RF government and almost certainly works for and was 'tasked by' the RF governments. See: United States Senate Committee on Intelligence, "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election - Volume 2: Russia's Use of Social Media." p. 5; Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," 2017. p. 4; Robert S. Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election," vol. I and II, 2019. pp. 19-35; EU vs Disinformation, "The St. Petersberg Troll Factury Targets Elections from Germant to the United States.," 2019, https://euvsdisinfo.eu/the-st-petersburg-troll-factory-targets-elections-from-germany-to-the-united-states/.

364 Christopher A. Bail et al., "Assessing the Russian Internet Research Agency's Impact on the Political Attitudes and Behaviors of American Twitter Users in Late 2017," *Proceedings of the National Academy of Sciences of the United States of America* 117, no. 1 (2020): 243–50. p. 243.

365 Ohlin, *Election Interference: International Law and the Future of Democracy*. pp. 28-29.

366 In echo chambers individuals are only exposed to information from like-minded individuals; in filter bubbles content is selected by algorithms according to previous on-line behaviour of the group or person, see: Eytan Bakshy, Solomon Messing, and Lada A. Adamic, "Exposure to Ideologically Diverse News and Opinion on Facebook," *Science* 348, no. 6239 (2015): 1130–32. p. 1130.

367 Aceves, "Virtual Hatred: How Russia Tried to Start a Race War in the United States." pp. 189-200.

368 A similar effect that is reached with targeted repression, see: Nugent, "The Psychology of Repression and Polarization." p. 12.

369 Anna Reynolds, *Social Media As a Tool of Hybrid Warfare, NATO Strategic Communication Centre of Exellence*, 2014. pp 28-31. Ong and Cabanes, "Politics and Profit in the Fake News Factory - Four Work Models of Political Trolling in the Philippine." p. 12.

targeted the US public and interfered in elections by persuading African American voters to boycott elections, encourage extremists to be more confrontational, and by spreading sensationalist, 'conspiratorial, and other forms of junk political news'.[370] For instance, the IRA-borne 'Blackivist' account, pretending to protest against the indiscriminate shooting of young black persons in the US,[371] was in fact intended to fuel societal division via social media.[372]

Trolling is often sensational in nature using headlines, emotions, pictures moving images, or virtual attacks on persons.[373] Trolling is a diffusional technique,[374] which leans more towards subconscious than conscious techniques. Since the aim is to deepen a divide, sowing discord is less needed, but deepening the discord is. Trolling content can therefore appear to be exaggerated or cynical. Trolling makes use of the heuristic association principle,[375] which refers to the concept that our brain looks for known information via associative relationships, patterns and coherences of data which reinforce stereotyping or stigmatisation. Trolling also uses heuristic anchoring and objectifying by which unknown phenomena become known.[376] Trolling can be so extreme that it loses effectiveness or even becomes counterproductive. [377] Trolling can be used to influence isolated (like-minded) groups, although this will only change their behaviour – making them more resolved - and not their values and beliefs. Isolated groups, especially those with an ideological character, are more susceptible to social heuristics techniques such as the use of credible and authoritative (virtual) actors.[378]

370 Howard, Kelly, and François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018." p. 3.

371 Amelia Acker and Joan Donovan, "Data Craft: A Theory/Methods Package for Critical Internet Studies," *Information Communication and Society* 22, no. 11 (2019): 1590–1609. Pp. 1600-1602; Ribeiro et al., "On Microtargeting Socially Divisive Ads: A Case Study of Russia-Linked Ad Campaigns on Facebook." pp. 142-143.

372 Howard, Kelly, and François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018." pp. 9-11. Blacktivist and 'BM' generating more than 500,000 followers, more than the genuine Black Life Matters movement, see also: Jason Parham, "Russians Posing as Black Activists on Facebook Is More Than Fake News," *WIRED*, 2017.

373 Vidya Narayanan et al., "Russian Involvement and Junk News during Brexit," *Comprop Data Memo 2017.10*, 2017.

374 Tansino, "Analysing Strategic Communications through Early Modern Theatre." p. 57.

375 Korteling, Brouwer, and Toet, "A Neural Network Framework for Cognitive Bias." p. 7.

376 Tansino, "Analysing Strategic Communications through Early Modern Theatre." p. 54. Anchoring is a way of making an unfamiliar element known by comparing or linking it to the reference system of the group – compare an unknown opponent to Hitler. Objectification is transforming an abstract notion into a concrete idea aligned with the reference system of the group – condense the rise and fall of the third Reich to Hitler.

377 United States Senate Committee on Foreign Relations, "Minority Report on Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security." pp. 19-20; Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." p. 29.

378 William D. Taylor et al., "Ideological Group Persuasion: A within-Person Study of How Violence, Interactivity, and Credibility Features Influence Online Persuasion," *Computers in Human Behavior* 51, no. PA (2015): 448–60. p. 455.

2.2.5.3. *Leaking of sensitive information*

Leaking is revealing[379] non-public information to the public domain with the purpose to harm an individual, organisation or a State.[380] Leaked information supports the strategic narrative in sowing discord, fueling fragmentation and spreading cynicism among the targeted audiences.

The leaking and abundant dissemination of retrieved non-public information into the public domain[381] does not necessarily use a false or manipulated content. Though during the 2017 French presidential elections the stolen data were altered, or additional information was added before leaking it (Macron Leaks).[382]

The main tool of influence for this cyber-related activity is not the content but the outlet of the information, making it difficult for the targeted audiences to assess the transparency and validity of the source. In the run-up to the 2016 US presidential elections,[383] State-controlled RF actors, including Sandworm and Fancy Bear,[384] hacked the Democratic National Congress and pilfered mail conversation, which was later disclosed via outlets such as DCLeaks and Wikileaks.[385] Releasing sensitive information induces the deflection to social and cognitive heuristics due to an overload of information and the subsequent inability to properly assess the data. Furthermore, the leak can also simulate a scandal, since the information was not intended for public consumption. The intent of the leak is to make 'deliberate attempts to direct public moral judgement against their target'.[386] Since the conscious human capacity to process cognitive data is limited, the focus is on consistency of data and whether they represent the truth or not. Inconsistency in the source or exposure of non-public data will confuse, deceive and astonish the targeted audiences.

379 Combined with an intrusion, the leak is part of doxing. When doxing is used as an offensive instrument it is called Doxfare (a word play on lawfare). Kilovaty, "Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information." pp. 149-152.

380 Sander, "Democracy under the influence: paradigms of state responsibility for Cyber Influence Operations on Elections", in *CJIL*, 2019, pp. 8-9. Whistleblowing is a sort of doxing operation.

381 Emilio Ferrara, "Disinformation and Social Bot Operations in the Run Up To the 2017 French Presidential Election," *First Monday* 22, no. 8 (2017). p. 3.

382 Erik Brattberg and Tim Maurer, "Russian Elections Interference: Europe's Counter to Fake News and Cyber Attacks," 2018. pp. 8-13; Shires, "Hack-and-Leak Operations: Intrusion and Influence in the Gulf." p. 238.

383 David P. Fidler, "The U.S. Election Hacks, Cybersecurity, and International Law," *AJIL Unbound* 110 (2016): 337–42. pp. 337-338.

384 These are so-called advanced persistent threats (APT). Both Sandworm and Fancy Bear (APT28) resorts under the RF military intelligence agency GRU and have been associated with hacks during US and French elections but also on private enterprises e.g. TV5Monde. APT29 (Cozy Bear) resorts under the general intelligence service. See also: FireEye, "APT28: A Window Into Russia's Cyber Espionage Operations?," Fire Eye Threat Research, 2014, https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html.; United States District Court, Indictment (United States v Andrienko) "Sandworm" (2020).

385 Jensen, Valeriano, and Maness, "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist." p. 220.

386 James Shires, "The Simulation of Scandal : Hack-and-Leak Operations, the Gulf States, and U.S. Politics," *Texas National Security Review* Fall (2020).

Leaks,[387] 'dumping',[388] kompromat[389] or white-wash operations[390] are often preceded by a computer intrusion – a hard-cyber hack,[391] though that is not necessarily executed by the same entity.

2.2.5.4. *Political Grooming*

Political grooming[392] refers to an influence activity to discredit (defamation)[393] or favour a political personality of some authority,[394] whether incumbent or prospective. Political grooming revolves around the concept of infiltrating politics by the cultivation of political allies',[395] and contains cyber-related activities, such as lobbying abroad,[396] foreign political advertising, party financing, purchasing advertisements (e.g. on Facebook),[397] supporting or manipulating minorities abroad on political issues.[398]

Political grooming can make use of fictitious (masqueraded) virtual persona on social media to influence targeted audiences.[399] These activities support the calibrated narrative and either use heuristics and biases including (political) advertisements on social media platforms or overwhelm the information environment with one-sided information in order to cause audiences to deflect to subconscious processing of information. Political grooming can also be initiated by domestic actors in, what Ohlin calls, soliciting foreign involvement.[400]

387 Such as during the 2016 US and the 2017 French presidential campaigns, See: Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election."; Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem."

388 Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 36 ff.

389 Bouwmeester, *Krym Nash: An Analysis of Modern Russian Deception Warfare*. p. 65; Kello, *The Virtual Weapon and International Order*. p. 222.

390 Mika Aaltola, "Democracy's Eleventh Hour: Safeguarding Democratic Elections Against Cyber-Enabled Autocratic Meddling," 2017. pp. 3-4.

391 Hack and Leak operations are also called 'doxing', see i.a. Jeangene Vilmer, "Information Manipulation: A Challenge for Our Democracies." p. 36. Doxing combines a hard- and soft-cyber operation.

392 EU vs Disinformation, "Election Meddling and Pro-Kremlin Disinformation: What You Need to Know." p. 4.

393 Martin and Shapiro, "Trends in Online Foreign Influence Efforts." p. 8. Also referred to as *ad hominem* attacks, see: United States Senate Committee on Foreign Relations, "Minority Report on Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security." p. 198; Rafal Modzelewski, "Virtual Togetherness : Sense of Identity and Community in Cyberspace," *Crossroads: A Journal of English Studies*, no. 1 (2013): 37–53. Para 2.4.

394 Jeangene Vilmer, "Information Manipulation: A Challenge for Our Democracies." p. 77.

395 Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict*. p. 83; Polyakova et al., "The Kremlin's Trojan Horses.", p. 3; Polyakova and Boyer, "The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition the New Geopolitics." p. 8.

396 Ajir and Vailliant, "Russian Information Warfare : Implications for Deterrence Theory." pp. 80-81.

397 Ohlin, *Election Interference: International Law and the Future of Democracy*. p. 18.

398 T S Allen and A J Moore, "Victory without Casualties: Russia's Information Operations" 4, no. 4 (2017). p. 68. Polyakova et al., "The Kremlin's Trojan Horses." pp. 3-6; United States Senate Committee on Foreign Relations, "Minority Report on Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security." p. 36.

399 Martin and Shapiro, "Trends in Online Foreign Influence Efforts." p. 24.

400 Ohlin, *Election Interference: International Law and the Future of Democracy*. p. 191.

Aaltola argues that 'a candidate, party, or a background group can create links and establish coordination with a foreign State to change the election dynamics' in order to synchronise efforts in tampering with the elections.[401]

The goal of RF political grooming, which is not confined to the information environment,[402] is aligned with the overall strategic concept of strategic confusion. By political grooming the RF often supports those parties, organisations or actors that amplify sowing discord, generate scattered political landscapes or increase division in a State, while increasing RF influence. The RF cultivates political extremes[403] by (financially) supporting specific (left-wing and right-wing) anti-establishment or anti-EU parties in Europe, such as Marine Le Pen's Front National,[404] the Austrian Freedom Party (FPÖ), the Italian League (Lega),[405] but also pro-Kremlin Swedish organisations such as Nordic Resistance.[406] Techniques are used to artificially boost the popularity or dismay of a candidate, using similar (semi) automated techniques for instance to increase the followers on Twitter and Facebook.[407]

Disinformation, trolling, leaking of sensitive information, and political grooming are cyber-related activities that aim to change the attitude and behaviour of the targeted State. These cyber-related activities are soft-cyber operations that use the content of messages as 'weapons'. During these activities, cyberspace is not changed or manipulated and will solely be used as a vector.

2.2.6. Exploiting Social Media: the feedback loop

Successful activities will need to be exploited. Similar to regular activities, whether military-type activities or marketing campaigns, after the thorough preparation and execution of a strategy, the output and the outcome will need to be assessed and evaluated and based on that new targets can be selected and exploited.[408] The latter is even more relevant for operations in cyberspace since many influence operations depend on ambiguous socially divisive topics

401 Aaltola, "Democracy's Eleventh Hour: Safeguarding Democratic Elections Against Cyber-Enabled Autocratic Meddling." p. 4

402 Laura Rosenberger and Lindsay Gorman, "Foreign Interference Is a Strategy, Not a Tactic," 2020.

403 United States Senate Committee on Foreign Relations, "Minority Report on Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security." pp. 50 ff.

404 Kragh and Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case." p. 775.

405 Polyakova et al., "The Kremlin's Trojan Horses." p. 4.

406 Kragh and Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case." pp. 801-803.

407 Isobel Cockerell, "How Russian Bots Amplify Britain's Jacob Rees- Mogg," *Codastory*, February 2019.

408 Similar to the so called OODA loop (observe, orient, decide, act) See: Frans P.B. Osinga, "Science, Strategy and War: The Strategic Theory of John Boyd" (University of Leiden, 2005). pp. 270-279.

and heuristics of the targeted audience and will therefore not have a predictable result[409] based on causal relations.[410] Nonetheless, the cyber-related activities that do catch on need to be exploited via a feedback-loop (see figure 2.12).

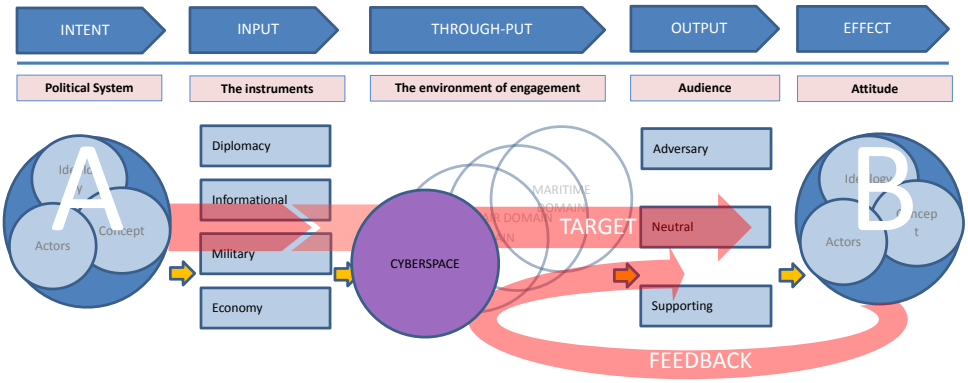

Figure 2- 12 The Feedback Loop

Social media, and especially the use of social media platforms via cyberspace,[411] can be exploited to enhance audience receptiveness and the effectiveness of the content of a cyber-related activity in two interrelated ways: by amplifying and magnifying messages, thereby creating the illusion of truth.

2.2.6.1. *Amplify & Magnify*

After preparing the influence operation, cyber-related activities depict the execution phase of the influence operations. Cyber-related activities that have an effect can be exploited by repeating the frame on multiple platforms and sites, so it 'is more likely to achieve a measure

409 Rid, *Active Measures: The Secret History of Disinformation and Political Warfare*. pp. 318-321. After the explosion of the Chernobyl Nuclear Power Plan in 1986, the KGB forged letters of the US Intelligence Services and leaked them to US newspapers. The latter did not pick up the story.

410 The concept that a change in attitude results in a change in behaviour is not uncontested. Ajzen and Fishbein argue that there is a causal sequence going from belief to attitude, social norm, intention and behaviour. Icek Ajzen and Martin Fishbein, *Understanding Attitudes and Predicting Social Behavior*, ed. Martin. Fishbein (Upper Saddle River, N.J: Prentice-Hall, 1980). Others, like Fointaint do not believe a clear causal relation exists but urge for more research on this topics. Valérie Fointiat and Laura Barbier, "Persuasion et Influence : Changer Les Attitudes, Changer Les Comportements. Regards de La Psychologie Sociale," *Journal d'interaction Personne-Système* 4, no. 1 (2015): 1–18. p. 1.

411 DeMarzo, Vayanos, and Zwiebel, "Persuasion Bias, Social Influence, and Unidimensional Opinions." p. 914; Cailin O'Conner and James O. Weatherall, *The Misinformation Age: How False Beliefs Spread* (New Haven [CT]: Yale University Press, 2019). p. 154.

of influence' with a specific targeted audience.[412] Repetition increases the availability of the topic to a wider audience, and facilitates the accessibility for specific audiences.[413] Repeating and magnifying cyber-related activities that affect target audiences will strengthen the beliefs of already polarised groups without swaying their positions, and may sow doubt to groups that have not yet taken sides.

Social media are well-suited for magnifying and amplifying the frames injected by cyber-related activities via echo chambers and so-called 'bots',[414] which are virtual persona that do not embody persons or groups but software applications. Bots are (semi-)automated algorithms which induce the fast diffusion or repetition of (false) messages via social media,[415] embodying the productive power of cyberspace as alluded to by Betz and Stevens.[416] The bots can be used to spread information with the purpose to saturating blogs and websites, overloading the information environment which facilitates the deflection to heuristics. Bots (algorithms or hybrid forms combining human activities and algorithms) used to intimidate or harass others on social media are also called trolls. Bots, other algorithms or people (governing numerous virtual persona) can repeat messages and content indefinitely with enduring persistency, in an anonymous way, without being restricted by scarcity of resources. [417]

The main difference between the traditional and digital ways of interstate influencing is that traditional targeting of audiences is directed at political elites or (a segment of) the population at large,[418] while the use of social media supported by micro-targeting techniques makes it possible to directly and remotely target groups, and even affect the individual, with adjusted tailor-made messages.

Communication in cyberspace is not dependent on a specific or a limited number of outlets. Influence operations in cyberspace, especially soft-cyber operations not only exploit

412 Renée Diresta and Shelby Grossman, "Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019" (Stanford, 2019). p. 8.

413 Chong and Druckman, "Framing Public Opinion in Competitive Democracies." p. 639.

414 Bot is short for the Czech word 'robotniks' (serf or workers) coined in 1921 by Karel Capek. See also: Freedman, *The Future of War: A History*. p. 233; Jeangene Vilmer, "Information Manipulation: A Challenge for Our Democracies." pp. 83-85; Scot Macdonald, *Propaganda and Information Warfare in the Twenty-First Century, Altered Images and Deception Operations*, 2007. pp. 83 ff.

415 Ohlin, *Election Interference: International Law and the Future of Democracy*. p. 19; Woolley and Howard, "Political Communication, Computational Propaganda, and Autonomous Agents: Introduction." p. 1, the authors define bots as: Bots are pieces of software intended to perform simple, repetitive, and robotic tasks. Bots are neutral in their performance, delivering news and information (real news as well as junk) or undertake malicious activities like spamming, harassment and hate speech. Whatever their uses, bots on social media platforms are able to rapidly deploy messages, replicate themselves, and pass as human users.

416 Betz and Stevens, "Power and Cyberspace." pp. 50-53. Productive power is diffusional and works through social relations. Cyberspace, thus Betz and Stevens, is ideally suited to the performance and transmission of productive cyber-power.

417 Fogg, *Persuasive Technology : Using Computers to Change What We Think and Do*. p. 7.

418 Dobber, "Data & Democracy: Political Microtargeting: A Threat to Electoral Integrity?" pp. 13-14.

social media regarding the content or form of the message, but also use the distributing mechanisms – the outlets – as opportunities for influencing in this new domain.[419] As a result content is no longer used as a means of communication, but the 'information deluge'[420] surges the public arena and undermines the discourse with one-sided arguments and messages. Consequently, the agenda-building function of societies may be frustrated or distorted. Assuming that social forces in society provide impetus to the political agenda, the one-sided denuding of the information sphere via a multitude of social media platforms could have a similar effect.[421] Gaining access to a multitude of social media platforms, and sharing one-sided arguments and political advertisements, disrupts the balance of the political dialogue, leading to a fragmented public sphere and hindering the ability to make informed political decisions.[422]

RF makes use of media outlets but also other relays including political and religious agents or fake NGOs,[423] thereby generating a 'permissive environment'[424] to disseminate the content. RF has substantive control over its national media outlets, such as Sputnik and RT broadcasting in many languages,[425] which creates a vast reach for disinformation and trolling messaging.[426] The message, spread by the State-run (social) media outlets, is amplified by proxy agents e.g. IRA and Fancy Bear, and magnified by a multitude of social accounts on Twitter and Facebook,[427] using both (semi) automated bots and human agents.[428]

419 Reynolds, *Social Media As a Tool of Hybrid Warfare*. pp. 23-24.

420 Lin and Kerr, "On Cyber-Enabled Information / Influence Warfare and Manipulation." p. 18.

421 Darren L. Linvill et al., "'The Russians Are Hacking My Brain!' Investigating Russia's Internet Research Agency Twitter Tactics during the 2016 United States Presidential Campaign," *Computers in Human Behavior* 99, no. May (2019): 292–300. pp. 293-294.

422 Judit Bayer et al., "Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and Its Member States," *Policy Department for Citizens' Rights and Constitutional Affairs*, 2019. pp. 16-17.

423 Martin and Shapiro, "Trends in Online Foreign Influence Efforts." p. 9; Jeangene Vilmer, "Information Manipulation: A Challenge for Our Democracies." pp. 70-72, see also Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses*. pp. 56 ff.

424 Allan, Haiden, and Reynolds, *Fake News. A Roadmap*. p. 64; United States Senate Committee on Foreign Relations, "Minority Report on Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security." pp. 24-31.

425 Elswah and Howard, "'Anything That Causes Chaos': The Organizational Behavior of Russia Today (RT)." pp. 629-632; United States Department of State, "GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem," 2020. pp. 14 ff; President Macron for instance stated, during a conference at Versailles in the presence of RF president Putin, 'On va se dire les choses: en vérité Russia Today et Sputnik ne se sont pas comportés comme des organes de presse et des journalistes mais comme des organes d'influence, de propagande et de propagande mensongère, ni plus ni moins', AFP, "A Versailles, Macron a Parlé Cash à Poutine Sur La Syrie, Les Droits de l'Homme Ou Les Médias Russes," *Le Point International*, May 29, 2017. See also: Jeangene Vilmer, "Information Manipulation: A Challenge for Our Democracies." p. 180.

426 Kragh and Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case." p. 781. RT was previously called 'Russia Today', and Sputnik formerly was 'the voice of Russia'; Allen and Moore, "Victory without Casualties: Russia's Information Operations." p. 67; United States Senate Committee on Foreign Relations, "Minority Report on Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security." pp. 40-46.

427 Twitter and Facebook are most used during RF influence efforts, followed by Instagram and YouTube, see: Martin and Shapiro, "Trends in Online Foreign Influence Efforts." p. 9.

428 Jeangene Vilmer, "Information Manipulation: A Challenge for Our Democracies." pp. 83-84; Martin and Shapiro, "Trends in Online Foreign Influence Efforts." Martin & Shapiro argue that in at least 50% of the RF foreign influence effort they

Platforms like Facebook are useful social media outlets for exploiting influence operations,[429] since news, opinions or other forms of information are shared not only based on political affiliations, but 'the flow of information on Facebook is structured by how individuals are connected in the network'.[430] Everyone can share his opinion,[431] views and emotions, as the price of admission to cyberspace is low. The exploitation of content on social media is non-hierarchical; it is an all-to-all way of communicating that is contagious,[432] attractive and rapid. Rid speaks about outsourcing communication in this context now that not only governmental agencies but everyone with a social media account is a communicator.[433]
The RF exploits social media to amplify disinformation, manipulate audiences, or gather data from individuals.[434] These cyber capabilities come at a low cost, can be easily distributed and accessed independently of geographical location, and activities are difficult to attribute not least due to the intermediary support of actors like Wikileaks or DCLeaks.[435]

2.2.6.2. *The illusion of truth*

The amplification of messages makes an abundance of data and information available and accessible to the targeted audience. The exposure to one-sided information can have the effect of overwhelming the public sphere, leaving little room for alternative opinions and beliefs. This effect is enhanced by the tendency of specific audiences to agree, support or 'like' the messages that like-minded audiences have sent. The amplification of (one-sided) messages will have the semblance of being truthful, candid or authoritive data.[436] Amplifying messages can underscore or even construct the proof for an occurrence, argument or happening, creating an illusion of truth.[437]

researched, automated accounts were used to spread data, pp. 8-9.

429 Hunt Allcott, Matthew Gentzkow, and Chuan Yu, "Trends in the Diffusion of Misinformation on Social Media," *National Bureau of Economic Research*, 2019. p. 3; Halberstam and Knight, "Homophily, Group Size, and the Diffusion of Political Information in Social Networks: Evidence from Twitter." p. 22.

430 Bakshy, Messing, and Adamic, "Exposure to Ideologically Diverse News and Opinion on Facebook." p. 1130.

431 Nissen, "#TheWeaponizationOfSocialMedia." pp. 43-49.

432 Robert J Shiller, "Narratives Economics," *American Economic Review*, no. 107(4) (2017): 967–1004. p. 4.; Bjarke Mønsted et al., "Evidence of Complex Contagion of Information in Social Media: An Experiment Using Twitter Bots," *PLoS ONE* 12, no. 9 (2017): 1–12. p. 10.

433 Rid, *Active Measures: The Secret History of Disinformation and Political Warfare*. p. 434.

434 Ajir and Vailliant, "Russian Information Warfare : Implications for Deterrence Theory." pp. 75-77.

435 William Banks, "State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0," *Texas Law Review* 95, no. 7 (2017): 1487–1513. p. 1489.

436 What Cialdini calls 'social proof', see: Cialdini, *Influence: The Psychology of Persuasion*. pp. 114 ff.

437 Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare." p. 22.

The illusion of proof is increased by using frames which often present fictitious connections and correlations which do not need to be true or reflect causality.[438] Cyberspace is inducive to exploiting the illusion. By using computational techniques the correlation (or random trends) between activities and occurrences can be fabricated, providing the suggestion of predictable behaviour.[439] Amplifying this correlation, without actually understanding the relation between occurrence and activity, via extensive repetition through social media will increase the illusion of truth[440] and consequently undermine the public discourse on societal issues. The illusionary element refers to the connections that remain hidden, but which create a fictitious causality.[441] Vicario et al. remark that '(m)any mechanisms cause false information to gain acceptance, which in turn generate false beliefs that, once adopted by an individual, are highly resistant to correction.[442] Or as DeMarzo et al. argue, repetition of statements increases the subject's belief in their validity, makes them more familiar, and familiarity serves as a cue to validity.[443]

This illusionary connection (and addictive inclination)[444] related to the number of, or the anticipation of receiving,[445] 'likes' can be exploited. RF uses social media algorithms to steer behaviour based on the number of likes, a social heuristic making humans support or comply with others if they feel familiar to or sympathise with them.[446] Using these biases, persons or groups will receive content that was 'liked' by persons with similar backgrounds or preferences.[447] Moreover, the system of 'clickbait' induces groupthink and -behaviour within virtual communities.[448]

438 A concept supported by the knowledge that the truth is not absolute but comes in 'degrees'. See: O'Conner and Weatherall, *The Misinformation Age: How False Beliefs Spread*. p. 30.

439 See e.g. Ziad Obermeyer et al., "Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations," *Science* 366, no. 6464 (2019): 447–53. pp. 1 & 6-7.

440 Constantly repeating content appeals to the cognitive heuristic of retainment, see: Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare." p. 22; but was previously reflected in the so-called Thomas theorem stating that "if men define situations as real, they are real in their consequences", see Thomas and Thomas, *The Child in America : Behavior Problems and Programs*. p. 572. The technique already used by Goebbels ('Wenn man eine große Lüge erzählt und sie oft genug wiederholt, dann werden die Leute sie am Ende glauben') but also used in the Lisa Case.

441 See also para 2.2.3.

442 Michela Del Vicario et al., "The Spreading of Misinformation Online," *Proceedings of the National Academy of Sciences of the United States of America* 113, no. 3 (2016): 554–59. p. 558.

443 DeMarzo, Vayanos, and Zwiebel, "Persuasion Bias, Social Influence, and Unidimensional Opinions." pp. 911-912.

444 P.W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (Houghton Mifflin Harcourt, 2018). p. 3. According to the author, every time a message is posted or a reaction ("like") received a burst of dopamine is released creating the need for another burst and hence another "like", or "tweet"; Peter Pomerantsev, *This Is Not Propaganda : Adventures in the War against Reality* (London: Faber & Faber, 2019). p. 161.

445 Barfman and Barfman, *Sway: The Irresistible Pull of Irrational Behaviour*. pp. 140-148.

446 Cialdini, *Influence: The Psychology of Persuasion*. pp. 167 ff.

447 Thomas, "Russia's Reflexive Control Theory and the Military." p. 245; Humans are receptive for positive emotions, and 'Likes' induce and accelerate the hunger for this sentiment, see Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare." p. 31, who speaks about the 'hedonistic treadmill'.

448 Ong and Cabanes, "Politics and Profit in the Fake News Factory - Four Work Models of Political Trolling in the Philippine." pp. 17-20; Bradshaw and Howard, "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation." p. 4.

Countering the amplified fabricated content with rational deliberation can have a counterproductive effect. During the 2017 French presidential election, Marine Le Pen used an anti-immigration narrative to persuade voters to support the Front National, thereby making use of real and fabricated news. Fact-checking reports by Le Monde, though, countervailed the false news used by Le Pen, or counter-narratives by other political parties trying to mitigate the issue, paradoxically increased the exposure of the immigration topic to the wider audience.[449]

Extensive social media exploitation will increase the impact of influence operations by augmenting the cyber-related activities via a feedback loop. Success, however, is difficult to measure. Referring to RF disinformation operations, Lanoszka states that campaigns are successful if they mislead the targeted audience into 'adopting beliefs that they would not otherwise have'.[450] Secondly, if the targeted State 'changes certain policies' which in turn shift the balance of power in favour of the RF.[451] Keir argues that the spread of the RF narratives on social media is already political gain in terms of knowledge and understanding of the RF position.[452]

Section 2.3.: Key Findings

'Speech is also a form of action'[453]
'Nothing is true and everything is possible'[454]

States generally co-exist in a peaceful and interdependent way. If, however, interests conflict, States may decide to act. One option for States is to employ influence operations in cyberspace. In this section the key findings are presented as an answer to the first sub-question of this research: *"What are the characteristics of influence operations, what mechanisms of influence can be applied and how does cyberspace affect influence operations."*

Influence operations in the context of this thesis are inherently soft-cyber operations. Operations in cyberspace can be divided in hard-cyber and soft-cyber operations. The former

449 Oscar Barrera et al., "Facts, Alternative Facts, and Fact Checking in Times of Post-Truth Politics," *Journal of Public Economics* 182 (2020). p. 18; Oscar Barrera et al., "Fake News and Fact Checking: Getting the Facts Straight May Not Be Enough to Change Minds," 2017.

450 Lanoszka, "Disinformation in International Politics." p. 242.

451 Lanoszka. p. 242.

452 Giles, "Handbook of Russian Information Warfare." p. 22.

453 Hannah Arendt, quoted in a Tweet by Samantha Rose Hill, see: https://twitter.com/Samantharhill/status/1341878966689345536

454 Peter Pomerantsev, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia*, First edit (New York: PublicAffairs, 2014). Front page.

target the virtual and physical dimension of cyberspace, generating effects in cyberspace. The latter use cyberspace as a vector applying content as the main 'weapon' to target the cognitive dimension. Soft-cyber influence operations favour the informational instrument of power, more specifically the strategic narrative.

The characteristics of influence operations can be best described as the deployment of resources for cognitive ends that foster or change a targeted audience's behaviour, directly or via a change in attitude.

To achieve this, influence operations utilises persuasive, compelling or manipulative forms of influence (see figure 2.13). With persuasive influence operations, State A aims to change the weight and number of options available to the targeted audience so that State B is voluntarily willing to make a choice that is beneficial to State A. Compelling influence operations short-cut or circumvent the deliberate understanding and autonomous decision-making process of the targeted audiences of State B, forcing them to consciously make an 'unwilling' choice. Whilst persuasive and compelling influence operations make use of rational and conscious techniques,[455] manipulative influence operations use subconscious techniques that subvert or usurp the autonomous decision-making process. The targeted audiences, often unaware of being influenced, are lured into making a reflexive biased judgment based on cognitive and social heuristics. Manipulation can be seen as a form of psychological compellence.

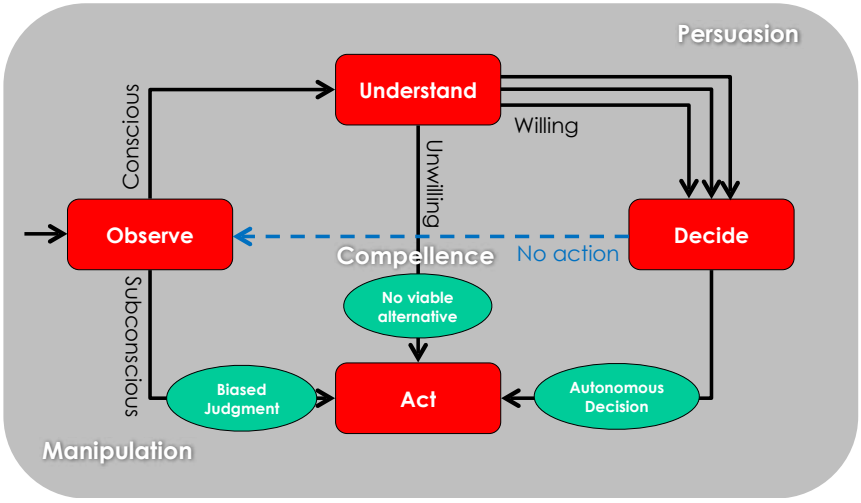

Figure 2- 13 Forms of Influence Operations

455 Kilovaty, "Legally Cognizable Manipulation." p. 469.

The aim of influence operations is to undermine the deliberate understanding and autonomous decision-making, or even to lure audience to make biased judgments. If audiences have biased judgments it means that they have been deflected from rationality and will use cognitive and social heuristics due to a time restraint, but more likely due to specific injects of framed content. Subconscious techniques, which force reflexive responses, circumvents the deliberate understanding and autonomous decision-making all together, thereby manipulating the target audience. The more influence operations rely on social and cognitive subconscious heuristics, the more they will shortcut or bypass deliberate understanding and autonomous decision-making, inclining or compelling to a biased judgment.

Influence operations, as strategies of States, follow a sequence of preparing, executing and exploiting. The preparation of influence operations starts with defining the intent, selecting the proper strategic narrative as an instrument of power, and operationalising the narrative in one of several frames.[456] Framing is the operational art of transforming strategic or policy aims (narrative) into actionable measures (cyber-related activities). A frame couples the strategic narrative to divisive topics of a society and audiences' preferences and heuristics around a specific event such as an election or the outbreak of Covid-19. The frames that are crafted do not need to be true. Depending on the way of influence – persuasive, compelling or manipulative - frames use conscious or subconscious elements to be receptive to the audience. The conscious elements, including socially divisive topics, are required to generate an air of realism to the frame, whereas subconscious heuristics and biases are needed to create reflexive responses. The more focus on the subconscious elements, the more manipulative the frame is. After preparation, the influence operation is executed via cyber-related activities such as spreading disinformation or trolling campaigns and, finally, exploiting successful activities via social media.

Though influence operations have been around for ages, cyberspace changes and affects influence operations and reinforces their effectiveness. The ICT environment and the social media platforms offer new opportunities to share and disseminate information with an unprecedented volume and accuracy.[457]

Cyberspace affects influence operations most prominently during the preparatory framing of the strategic narrative, and in facilitating the deflection towards subconscious heuristics via the cyber-related activities via social media during execution and exploitation phase.

456 Regarding the stages of influence operations, see also: Aaltola, "Democracy's Eleventh Hour: Safeguarding Democratic Elections Against Cyber-Enabled Autocratic Meddling." pp. 3-4; Jeangene Vilmer, "Information Manipulation: A Challenge for Our Democracies." p. 83; Rid, *Active Measures: The Secret History of Disinformation and Political Warfare*. p. 5; Jean Baptiste Jeangene Vilmer, "Lessons from the Macron Leaks," in *Hacks, Leaks and Disruptions*, ed. Nicu Popescu and Stanislav Secrieru, 2018. pp. 75-76.

457 Barela and Duberry, "Understanding Disinformation Operations in the 21 St Century." p. 41.

Cyberspace and especially computational sciences make it possible to generate extensive algorithms and (correlation) knowledge regarding the audiences and society by excavating data on the Internet and social media. The data can be used to pinpoint socially divisive topics, preferences and heuristics of specific groups within society. Conversely, the data in the virtual dimension of cyberspace make it possible to micro-target and single out certain groups in society with tailored messages based on the data regarding their behaviour and beliefs. The content of the bespoke messages audiences obtain may have the aim to sow discord (disinformation), exacerbate polarisation (trolling), favour or undermine actors (political grooming), or create a shock-and-awe effect by leaking non-public information to the public domain.

The characteristics of cyberspace and social media also make it possible to create an overload of information, generate a sense of urgency for decision-making, and generate algorithms that create confusion, thereby hindering the possibility to give meaning to the data provided. Cyberspace is, therefore, conducive to deflecting the rational mind toward cognitive and social heuristics resulting in biased judgments. Influence campaigns can deliberately exploit social media to magnify and amplify specific messages to which the audience is receptive. Due to the velocity and reach of the Internet, the exploitation of successful cyber-related activities runs parallel with the cyber-related activity, reinforcing the effect and exacerbating the information overload and inability to make sense of the proffered data.