BRILL
NIJHOFF

SECURITY AND HUMAN RIGHTS 29 (2018) 3-23

SECURITY AND
HUMAN RIGHTS
brill.com/shrs

Disinformation in International Relations: How Important Is It?

André W.M. Gerrits
Professor of International Studies, Institute for History, Leiden University
a.w.m.gerrits@hum.leidenuniv.nl

Abstract

This article explores the relevance of disinformation in international relations. It discusses the nature of information manipulation, ways to counter disinformation, and possibilities for international organizations, including the OSCE, to initiate confidence-building measures. The article suggests that although disinformation becomes an increasingly salient aspect of global politics, its security impact should not be overstated. As in domestic politics, international disinformation parasites on existing divisions and concerns, which it exploits rather than creates. This should not be trivialized. Disinformation is disruptive and it further deteriorates the overall international context. But as yet it is not a significant security challenge, and it does not change the international balance of power.

Keywords

disinformation – international relations – confidence-building-measures – Russia

1 Introduction[1]

'Information has been weaponized, and disinformation has become an incisive instrument of state policy', according to a recent 'White Paper' by the US Department of Defense and the Joint Chiefs of Staff that singles out the role of

1 I am thankful to Max Bader for giving me access to his extensive electronic data base on international information manipulation.

information in international relations.[2] The report specifies how in relations among states information and disinformation have not only fundamentally changed ('weaponized') but have also become much more critical ('incisive'). A recent Oxford University inventory of organized information manipulation compares 28 countries that engage in these information activities.[3] Among these countries is Russia. Allegedly, few other countries are as deeply involved in 'information warfare' as Vladimir Putin's Russia is. There are good reasons to focus on Russia's international information manipulation, but there is even more reason to emphasize that Russia is far from the only country that engages in these activities. Information manipulation has become a global phenomenon, a prominent instrument in the strategic foreign policy toolkit of a great deal of governments, at bilateral, regional and global levels.

This contribution will take a closer look at the impact of disinformation on relations between states, especially within the area of the Organization for Security and Cooperation in Europe (OSCE), and among its member states. Is the manipulation of information as novel and as threatening as the US White Paper and an impressive array of other publications suggest? Literally hundreds of studies on disinformation generally and on information manipulation by Russia specifically have been published during the last few years, by academic institutions, think tanks and international governmental organizations. But how important is disinformation really? And if it is as significant as many suggest, how to effectively counter it? How have national governments and international organizations, including the OSCE, responded to the threat? States seem to have relatively effectively dealt with earlier technological challenges, nuclear weapons included. Will they also be able to tame the potentially subversive impact of information and communication technology?

2 Disinformation in International Relations

Disinformation in the context of international relations concerns the deliberate spread of false or unbalanced information by foreign states (or relevant

2 M. Severin, 'Russian Activities in Africa (Continued)', in United States Department of Defense and Joint Chiefs of Staff, *Russian Strategic Intentions. A Strategic Multilayer Assessment* (*SMA*) *White Pape,* (Washington, DC, May 2019), 70–71, https://nsiteam.com/sma-white-paper-russian-strategic-intentions/. (All websites referred to in this article were retrieved in May–June 2019.)

3 S. Bradshaw and Ph. N. Howard, *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*, University of Oxford, Working Paper no. 2017.12, https://comprop.oii.ox.ac.uk/research/troops-trolls-and-trouble-makers-a-global-inventory-of-organized-social-media-manipulation/#iLightbox[gallery1587]/0.

non-state actors[4]) with the primary objective to confuse and mislead, to sow disagreement and discord among parts of the population in other countries. The disinforming state's goal is to strategically benefit from other government decisions which results from these disagreements, and to ultimately increase one's own relative international influence. In international relations, disinformation or information manipulation is an instrument of foreign policy. All other aspects of information manipulation, among other things disinformation aimed at domestic audiences, by independent non-state actors, or for commercial or amusement purposes, are left undiscussed in this contribution. Disinformation as an instrument of foreign policy can be part of a much larger, much more dangerous complex of international state-led activities in cyber-sphere, including cyber-attacks, hacking and other subversive activities that are often shared under the rather confusing notion of 'hybrid warfare'.[5] Hybrid warfare refers to the full spectrum of war activities, with the exception of full-scale military conflict. War comes with disinformation; but disinformation is not necessarily war. This contribution discusses disinformation only. Other aspects of hybrid warfare are left undiscussed.

Disinformation is an age-old aspect of foreign policy and warfare. But it is different today. It is technology, more than intent or content that makes disinformation today rather unlike earlier forms of international information manipulation. Disinformation is not limited to, but it proliferates especially via social media. This largely determines its speed, its reach, and its impact. The basic technique of international disinformation is well-known. Computational systems incentivize and automate media content in ways that result in broader, but also in more focused circulation. Commercial incentives can lead to further spread of unverified and fabricated stories of a political relevance. Hackers, trolls, honey-pots, bots, fake accounts on digital networks, fake grass-roots user groups (astroturf) and all other 'actors' in the digital sphere flood social media are involved in spreading biased and fake messages and other

4 There are two types of non-state entities active in the field of international disinformation: independent, non-state affiliated organizations that act out of political and ideological beliefs (ISIS, Al-Qaeda being the most well-known examples) and private or semi-private, sometimes commercial organizations that openly or covertly work for the state.

5 For a sober analysis of hybrid power and warfare, especially in the case of Russia, read M. Galeotti, 'Hybrid, Ambiguous, and non-linear? How New is Russia's "New Way of War?", *Small Wars and* Insurgencies, 27, 2016, 2, 282–301, http://dx.doi.org/10.1080/09592318.2015.1129170. For an excellent introduction on the transforming nature of 'cyber space' on international relations, see L. Kello, *The Virtual Weapon and International Order*, New Haven and London, Yale University Press, 2017.

manipulated information content.[6] When state-actors are involved in any of these activities, and when the manipulation of information is deliberately aimed at foreign audiences, we refer to disinformation as an aspect of international relations.

Disinformation by foreign states and relevant non-state actors is routinely presented as a major threat to Western democracies and to the international institutions which they built.[7] Awareness of the danger of information manipulation for political purposes rose sharply after repeated foreign interferences into the domestic policy process of Western countries, especially during election campaigns. The most notorious cases are the American presidential elections (2016), Brexit (2016), the referendum in the Netherlands on the EU Association Agreement with Ukraine (2016), and the attempted intervention in the French presidential elections in 2017, including the 'Macron Leaks'. A series of incidents in other European countries (and from other parts of the globe), especially in the former Soviet republics of Ukraine (the unofficial epicentre of international information manipulation) and the Baltic States, added to the international alarm. And there is an additional reason why disinformation is widely considered as a danger to democracy, and that is the current state of democracy itself. Political polarization, declining trust in the institutions of representative democracy, the rise of strongmen politics—the potential impact of disinformation adds to the widespread feeling that liberal democracy is under pressure.

Even though it is not difficult to imagine that disinformation may serve the foreign policy interests of states (as it has always done), it is far from easy to identify and expose it. Information manipulation campaigns often combine elements of disinformation with misinformation (information that is unintentionally inaccurate) and truthful information.[8] It proves difficult to trace

6 J.A. Tucker, et al., *Social media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature*, William and Flora Hewlett Foundation, Menlo Park, Ca., March 2018, https://hewlett.org/library/social-media-political-polarization-political-disinformation-review-scientific-literature/ gives a well-informed overview of these disinformation tactics and their potential impact on democratic policy processes.

7 The link between disinformation and the weakening of democratic society is not undisputed, but still frequently mentioned in major studies on international disinformation. See especially: Tucker, op. cit. and J.-B. Jeangène Vilmer, et al., *Information Manipulation: A Challenge for Our Democracies, Report by the Policy Planning Staff* (CAPS) *of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research* (IRSEM) *of the Ministry of Armed Force*, Paris, August 2018.

8 C. Jack, *Lexicon of Lies: Terms for Problematic Information,* Data and Society Research Institute, New York, September 2017.

the origins, the source, of a given piece of disinformation, and it is even more problematic to establish the political actors and intentions behind it, the 'attribution'-factor. But especially in relations among states the attribution issue is crucial. If origin and intent can be suspected but not proven, and this appears to be the case in many instances, responses that go beyond purely defensive measures are problematic, because they will inevitably increase rather than reduce international tension.

Disinformation in relations among states is not the preserve of any country or political order in particular, and neither is it a typically modern or novel phenomenon. In a recent report *Freedom House*[9] registered two simultaneous, and probably not unrelated trends: a decline in internet freedom (China being the worst abuser for the third consecutive year) and an increase in disinformation activities. Among the 65 countries surveyed, more than thirty states engaged in disinformation and influencing activities within and beyond their own borders. Disinformation played a role in elections in at least eighteen states.[10] Democracies usually have a full range of checks and balances, which are largely absent among authoritarian governments. These checks and balances neither protect democracies against disinformation, nor do they prevent them from engaging in international disinformation activities. But they do make it more difficult to hide disinformation campaigns or to repress public discussion. One may therefore reasonably assume that the manipulation of information for foreign policy purposes is particularly pertinent in the case of non-democratic, authoritarian regimes.

In this context there is no other country that attracts as much attention as Russia does. The European Commission, which considers disinformation as 'a major challenge' for Europe,[11] identifies Europe's major non-democratic power, Russia, as the 'greatest threat'. The Commission defines Russia's disinformation campaigns as 'systematic, well-resourced, and on a different scale to other countries'.[12] Many researchers and institutions share the Commission's interpretation. Russia is singled out as the main perpetrator in what is

9 Freedom House, *Freedom on the Net 2017. Manipulating Social media to Undermine Democracy,* N.p., n.d., https://freedomhouse.org/report/freedom-net/freedom-net-2017.

10 See the contribution by Max Bader to this issue of *Security and Human Rights*.

11 European Commission, *Joint Communication to the European Parliament, the European Council, the Council, The European Economic and Social Committee and the Committee of the Regions: Tackling Online Disinformation: A European Approach.* Brussels, 26.04.2018, COM(2018) 236 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&from=EN.

12 European Commission, *Joint Communication to the European Parliament, the European Council, the Council, The European Economic and Social Committee and the Committee of*

often perceived as an international information war, aimed at influencing and undermining the domestic political processes in multiple countries.[13] Consequently, Russia's international disinformation activities have been widely studied and they are relatively well-documented.[14]

If one takes as an indication this large number of recent governmental, think tank and academic publications on disinformation, and the range of institutions that have been set up to detect and counter it, disinformation may seem to be an exceptionally powerful phenomenon. The fact that it proves nearly always impossible to measure the impact of disinformation on a target state's domestic or foreign policies, makes this fixation, especially with the manipulation of information by Russia, all the more remarkable. But perhaps it is precisely this aspect of political uncertainty, in combination with the rapidly evolving and for many difficult to grasp high-tech dimension of disinformation, that makes it such an intriguing and widely-discussed issue. But does this massive interest in international disinformation campaigns warrant its actual significance? Disinformation is not an end in itself; it is supposed to serve a larger political objective. Concretely, in the case of Russia, through provoking changes in the behaviour of other states, disinformation is expected to influence the 'correlation of forces' into Russia's advantage. Russia seeks a strategic benefit through the international manipulation of information. Is there reason to believe that the Kremlin actually meets its ambitions? Can we realistically establish the weight and effectiveness of Russian information manipulation in international relations today?

---

the Regions. Action Plan Against Disinformation. Brussels, 5.12.2018, JOIN(2018). 36 Final, https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf.

13 A major French study on disinformation assert that its interlocutors among European authorities attribute 80 percent of foreign influencing efforts in Europe to Russia (Jeangène Vilmer, op. cit., p. 49). See also the contribution to this special issue by Uladzidlau Belavusau on disinformation and memory laws in Poland and Ukraine, two target countries for Russian disinformation campaigns.

14 There is a huge amount of studies on Russia's alleged disinformation activities. Especially informative are: T.C. Helmus et al., *Russian Social Media Influence. Understanding Russian Propaganda in Eastern* Europe, Santa Monica, Calif., RAND Corporation, 2018; Jeangène Vilmer, op. cit.; et al.; P. Pomerantsev and M. Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture, and Money: A Special Report Presented by the Interpreter, a Project of the Institute of Modern Russia*, Institute of Modern Russia, 2014, https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf.

3 Disinformation and Russia's Foreign Policy

Although Russian disinformation activities seem especially tangible in its neighbouring countries, where minority groups can be relatively easily reached, Russian-language media is plentiful, and powerful (non) state organizations are active as potential proxies (Ukraine, the Baltic States), no single case is better documented than Russia's interference in the American presidential elections of 2016.[15] Disinformation activities that can be credibly traced back to Russia, are almost automatically linked to the country's political leadership. In other words, in the case of Russia, information manipulation is almost routinely interpreted as *political* disinformation. It is seen as part of the country's strategy to undermine the political process in Western democracies and to influence these democracies' external relations. There is no doubt that Russia-related activities in the sphere of information manipulation are vast. This is credibly shown by the large number of publications and web sites that aim to map out, debunk and counteract these efforts.[16] But how effective is the manipulation of information from Russia?

As do most governments, the Russian leadership considers information as an important aspect of international relations and geopolitical competition. Ideas and beliefs are seen as key features of global politics and, in line with the realist interpretations of international relations, ideational influence is believed to support material power, and vice versa. Russia's recent security doctrines all refer to the increasing relevance of information in international relations. After a brief flirt with democratic and political-economic liberal values during the early Yeltsin years, from the mid-1990s the critical part of the Russian leadership perceived the spread of these norms, values and their related political institutions as a threat to Russia. During the first two decades after the Cold War, the West reigned supreme in this global ideational competition, and Russia took a mostly defensive posture. Today, Russia rides on the anti-liberal wave that it helped to initiate, and it self-confidently works to weaken the Western, Anglo-Saxon dominance in the global sphere of information.

15 Special Counselor Robert Muller did not find evidence of collusion between members of the Trump campaign team and representatives of the Russian government, but his investigations confirmed that Russia interfered in the 2016 American presidential elections in a 'sweeping and systemic fashion', by stealing and disseminating personal emails and by widely spreading disinformation. See R.S., Muller, III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election.* Washington, D.C., March 2019, p. 9, https://www.documentcloud.org/documents/5955118-The-Mueller-Report.html.

16 See footnote 14.

Official doctrines show both the defensive and the offensive dimensions of Russia's information strategy. The country's recently adopted doctrine on information security (December 2016) emphasizes the detrimental impact of information manipulation on international security and stability, and on Russia itself. It talks about 'a growing information pressure on the population of Russia (…), with the aim to erode Russian traditional spiritual and moral values'.[17] This becomes all the more acute, the doctrine critically argues, because Russia's own information industry depends so much on foreign technology.[18] Russia's latest Military Doctrine (2014) takes a more bellicose position. It presents information and communication as important features of 'modern warfare'. Russia *must* engage in this war, the doctrine asserts, for defensive *and* for offensive purposes.[19]

For the Russian leadership, disinformation has become a matter of established policy. It is a relatively simple, increasingly precise, and comparatively inexpensive method to reach important strategic goals. There is much to win politically, and little to lose. Peter Pomerantsev and Michael Weiss[20] suggest that Russia's influence through disinformation can be considered as concentrical: Moscow can generate chaos in Ukraine, destabilization in the Baltic States (part of a larger effort to influence and protect the perceived interests of Russian-speaking people in former Soviet republics), political influence in Eastern Europe, confusion in Western Europe, and distraction in the United States. Information manipulation by the Russian state has been characterized as part of a 'sophisticated set of gray zone tactics of "asymmetric balancing" through which Russia pursues its strategic ends within relatively limited means.'[21] The notions of asymmetry and balancing are key. They explain the apparent discrepancy between Russia's relatively limited 'objective' power instruments and the global influence which it allegedly pursues. In 2018 Russia's GDP in current US dollars was less than one-tenth of the size of the economy

17 *Doktrina Informatsionnoi Bezopasnosti Rossiiskoi Federatsii*, December 5, 2016, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=ru_RU.

18 Idem.

19 *Voennaia Doktrina Rossiiskoi Federatsii*, *Rossiiskaia Gazeta*, December 30, 2014, https://rg.ru/2014/12/30/doktrina-dok.html.

20 Pomerantsev and Weiss, op. cit., p. 24.

21 R. Person, 'Russian Grand Strategy in the 21st Century', in United States Department of Defense and Joint Chiefs of Staff, *Russian Strategic Intentions*, *A Strategic Multilayer Assessment* (SMA) *White Paper,* Washington, DC, May 2019, https://nsiteam.com/sma-white-paper-russian-strategic-intentions/, p. 7.

of the US or the European Union.[22] In that same year, the United States spent ten times more on defence than Russia did, and its defence budget accounted for a lesser share of GDP than Russia's military expenditures.[23] In other words, and this may sound rather counter-intuitively, the use of disinformation as a foreign policy tool by Russia, is a high-tech, poor man's strategy.

Many observers emphasize the difference between propaganda from the Soviet period and disinformation today. Russia's current foreign information strategy is mostly interpreted as negative. Russia's aim is not so much to preach and convert through the dissemination of its own points of view, its own ideas and ideologies (as it did in communist times), but to confuse and weaken, through the spread of biased, false or simply as much 'information' as possible. This distinction seems only partly right. True, Russia's prevailing idea is to confuse, rather than to convert. But if Russia exercises influence beyond its borders, it is probably not only because of 'negative' propaganda or disinformation only. There is a new dimension to Russia's international appeal. For the first time in decades, the country exercises soft power in the West.[24] Russian interference in electoral processes or its more general attempts to influence political developments in Western countries benefit from the fact that local political forces are evidently sympathetic to Russia, to its leadership, and to the political values and ideas that it claims to stand for. Western political actors are willing to listen to Russia, and to cooperate with it.[25] Putin has successfully brand-named Russia as a conservative bastion against the excessive political, economic and cultural liberalism of the West. People recognize and appreciate in Russia what they dislike, hate or miss in their own societies. In that sense, the perceptions of Russia tell us more about ourselves, than about Russia. It is the latest variant of an age-old tradition: Russia as the counter-image of the West.[26]

---

22 World Bank Group, Databank, 2019, https://data.worldbank.org/indicator/ny.gdp.mktp.cd?locations=ru.

23 SIPRI, *Trends in World Military Expenditure,* 2018, Stockholm, April 2019, https://sipri.org/sites/default/files/2019-04/fs_1904_milex_2018_0.pdf.

24 My argument is *not* that international disinformation or information manipulation is a form of soft power; my argument is that the level of attractiveness that Russia enjoys make some Europeans more susceptible to the country's disinformation campaigns than they would otherwise be.

25 In recent years, the Freedom Party in Austria and the League in Italy signed cooperation agreements with the Kremlin-dominated 'United Russia' party.

26 Read the impressive and still topical study by M. Malia, *Russia under Western Eyes: From the Bronze Horseman to the* Lenin Mausoleum, Cambridge, Mass., Belknap / Harvard University Press, 1999.

Russia exercises soft power, and not just among some countries of the Former Soviet Union, but also in the West. This makes it even more difficult to neatly distinguish between disinformation and other forms of manipulation on the one hand and public relations, public diplomacy and even political affinity on the other. Vladimir Putin's blend of nationalist, conservative, anti-globalist, anti-liberal, anti-Western elitist, and anti-immigration discourse strikes as rather opportunistic for a politician who until relatively recently prided himself as pragmatic and non-ideological, but it seems to work. It proves relatively effective among his own citizens and it works among parts of the population in Europe and elsewhere.

Various political parties from the 'left' and from the 'right' in the countries of the European Union embrace (some of) the political values that Russia has come to propagate. Russia, or rather the policies of the Russian leadership, are seen in a positive light by a substantial minority of Europeans and Americans. A recent publication gauged this segment of Europe's party-political landscape as 'non-mainstream but significant'.[27] Most of Russia's friends in Europe belonged to the political fringe. But the fringes of politics in Europe are moving, and they have become increasingly fluid. Russia sympathizers come in many shapes and forms. The *Russlandversteher* in Germany belong to the more moderate variant. They are driven by a combination of historical guilt and responsibility and a strong sense of their country's special position towards Russia (geopolitically and economically). There are *Russlandversteher* in all of Germany's political parties, and in most European countries—individuals and parties who believe that it is in the security interest of Europe to find ways to cooperate with Russia, rather than to continue to antagonize it.[28] They share some international interests with the Russian leadership, without feeling much affinity with its ideological world outlook. It is of importance to distinguish the Russia sympathizers from Russia's friends. The latter are a relatively new phenomenon (since Moscow-loyal communists became extinct): political parties

27 St. Braghiroli and A. Makarychev, 'Russia and its Supporters in Europe: Trans-ideology à la carte?', in *Southeast European and Black Sea Studies*, 16: 2, 213 (DOI: 10.1080/14683857.2016.1156343). For Russia's proxy groups in the former Soviet Union, especially Ukraine, Georgia and Moldova, where Russia's influence, through hard and soft power means, is generally stronger: O. Lutsevych, *Agents of the Russian World. Proxy Groups in the Contested Neighbourhood,* Research Paper, Russia and Eurasia Programme, Chatham House, London, 2016.

28 I could well imagine that this feeling grows, now that trust in the leadership of the United States among Europeans seems under increasing pressure. I am not aware though of recent figures that causally link the two political sentiments: distrust in the United States and rapprochement towards Russia.

that share ideological affinity with Russia and that use their relations with the Kremlin to further their own political ambitions. But the list is growing: Front National, the Freedom Party of Austria, Orban's FIDESZ party, Salvini's Lega, and quite a few more.[29]

The relative prominence of Russia's friends in Europe is a nuisance for those who disagree with their ideas, but as yet, they do not represent a serious threat to Europe's political mainstream. And if they ever will, which is not inconceivable, it will not be because they enjoy the ideological and occasionally the financial support of the Kremlin, but because they represent the perceived interests of a significant part of their countries' electorates. Russia has political friends in Europe, but in terms of soft power projection it still has a long way to go. A recent 25-country poll by the Pew Research Center finds that 70 percent of the respondents believe that Russia plays a more (42 percent) or as important role (28 percent) in world politics today compared to ten years ago; while only 34 percent express a favourable view of Russia generally (54 percent negative). Confidence in Putin is even lower: 26 percent positive against 63 percent negative.[30] With or without Putin, Russia's global reputation is still relatively poor. Many may appreciate Russia as a counterweight to an arrogant, overbearing West; few however admire it for either its own socioeconomic or political domestic order. Russia may be a friend, but it is not a model.

4 How to Counter Disinformation?

To effectively counter international disinformation, one needs to first recognize it, then to identify its origins and to prove intent, and finally to effectively neutralize it. Every step of the process is problematic. Obviously, given that international disinformation is mostly aimed at exploiting existing rifts and tensions, the most effective political counter-strategy would be to take away the causes of these problems. Otherwise, there is no silver bullet for countering international disinformation. In the end we will need to learn to live with it.

More targeted responses to disinformation fall into four non-mutually exclusive categories.[31] Responses can be primarily 'educational', making people

29 Braghiroli and Makarychev, op. cit.

30 *Image of Putin, Russia Suffers Internationally*, Pew Research Center, Global Attitudes and Trends, December 6, 2018, https://www.pewresearch.org/global/2018/12/06/image-of-putin-russia-suffers-internationally/.

31 Particularly informative literature on possible counter-strategies: Jeangène Vilmer, op. cit.; *A Multi-dimensional Approach to Disinformation. Report of the Independent High-Level*

more resilient to disinformation. They can be 'protective', using high-tech means to detect and counter disinformation.[32] They can be 'repressive', using technologies to block the manipulation of information. And they can be 'political', trying to reach a sense of understanding among states on the subversive impact that disinformation may have on international trust and security, and therefore aiming to find ways to 'tame' it, for example through the development of confidence-building measures (CBMs).

The educational approach aims to raise information awareness and to debunk information manipulation through a combination of increasing media literacy, fact-checking, defining standards of information accuracy, and promoting a clear, coherent, entertaining and convincing counter-narrative. Education is the least offensive response, perhaps also the most effective one, but unfortunately, it is also the most difficult and time-consuming answer to disinformation.

Disinformation exploits existing differences in target societies. Given that lack of trust in media and government is arguably one of the major reasons why people become more susceptible to disinformation, media campaigns by governments and other initiatives by (semi-)official institutions, such as labels, indexes and rankings that are supposed to distinguish reliable media from untrustworthy ones, may not be particularly effective. Governments and other political actors are often party to the differences that they attempt to address. One may expect that those groups that are vulnerable to foreign disinformation cannot be easily reached and convinced by their national governments, and probably less so by international organizations, including the European Union. Many people actively seek the type of information that governmental counter-strategies attempt to neutralize. This type of counter-strategies may therefore actually increase the attractiveness of extreme and heavily biased information. Disinformation seem especially effective, where and when political opinions are already polarized. Disinformation confirms rather than challenges pre-existing ideas—a phenomenon known as 'confirmation bias'. The manipulation of information strengthens the echo chamber effect of beliefs and ideas. A significant number of citizens seek no access to other forms of

Group on Fake News and Online Disinformation, March 2018, https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation, commissioned by the European Commission.

32 See the contribution on artificial intelligence and disinformation by Katarina Kertysova, with Eline Chivot in this issue.

knowledge and information, and prefer to continue to live in their own 'alternative reality'.[33]

Partially depending on the actual threat perception, national governments have taken a range of specific measures; they have established a plethora of networks, working groups, task forces, strategic communication units and other institutions. Some governments have issued legal acts and codes of practices concerning disinformation; others have taken steps to engage social media platforms in co-regulatory activities.[34] In the context of international relations, the response by international organizations is particularly relevant, and in this realm the European Union has clearly taken the lead.

'(T)o gain a more comprehensive, regular and reliable picture of Russia's disinformation campaign' is the main objective of the European Union's East StratCom Task Force, established in 2015 on the initiative of the European Council. The Task Force arguably is the EU's most important initiative in its counter-disinformation efforts, especially also in the countries of the Eastern Partnership.[35] A few dozen of full-time and seconded staff and an army of

33 The quote comes from St. Lewandosky, U. Ecker, and J. Cook, 'Beyond Misinformation': Understanding and Coping With the "Post-Truth" Era', in *Journal of Applied Research in Memory and Cognition*, 6, 2017, 4, p. 360. I am not sure if 'alternative reality' applies only to the part of the population that is particularly susceptible to disinformation or that it applies to other groups in society as well. Other publications qualify the echo chamber effect of social media use (see C. Wardle and H. Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, Council of Europe report DGI (2017), Strasbourg, October 2017, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c).

34 For the wide variety of national responses, see: *Disinformation and Propaganda—Impact on the Functioning of the Rule of Law in the EU and its Member States.* Brussels: Policy Department for Citizens' Rights and Constitutional Affairs, Directorate General for Internal Policies of the Union, February 2019 http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf ; M. Hellman and Ch. Wagnsson, 'How can European States Respond to Russian Information Warfare? An Analytical Framework', European Security, 26, 2017, 2, 153–170 (DOI: 10.1080/09662839.2017.1294162). The *European* approach to tackling disinformation essentially aggregates this variety of initiatives (See 'EU-Wide Code of Practice on Disinformation' (Brussels, September 2018). For the link to this code: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation).

35 Related initiatives by the European Union are the 'Hybrid Fusion Cell' and the 'European Centre of Excellence for Countering Hybrid Threats', set up by The Joint Communication on Countering Hybrid Threats within the European External Action Service. The EU considers disinformation campaigns as potential vehicles for hybrid threats. See European Commission, 5.12.2018. JOIN(2018), op. cit.

volunteers scour the internet for disinformation messages and related content, and feed into the Task Force's website and its weekly *Disinformation Review*.[36] The European Council in December 2018 commended the work done by the Task Force and especially the uncovering of 'numerous disinformation narratives' by the Russian Federation.

NATO and EU largely overlap in membership and in threat perception, and so do their responsive measures against disinformation. In its *Action Plan Against Disinformation* the European Commission mentions NATO and the Group of 7 as its 'key partners' in the effort to combat the manipulation of information and to protect the democratic system.[37] It is difficult though to get a clear picture of the level of international coordination and synchronization. The Strategic Communication Excellence Centre (StratCom CoE, in Riga) is NATO's flagship organization, whose activities seem more offensive but otherwise not essentially different from what the EU's StratCom Task Force is doing.[38]

The Council of Europe and the OSCE are less active in the international effort to counter disinformation than NATO and especially the EU. The Council of Europe commissioned a highly informative study on 'information disorder'[39] and its Parliamentary Assembly expressed concern over the increase in online media disinformation campaigns,[40] but like the OSCE it tends to approach information manipulation primarily as a challenge to the freedom of information, rather than as a destabilizing aspect of relations among states.

The OSCE is an all-European organization, concerned with human rights and international security, which includes the membership of the United States and Russia. At first glance, it would be an ideal institution to address the issue of disinformation and to develop common responsive strategies and

36 Information from the website of StratCom's host institution, the European External Action Service, https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en.

37 European Commission, *Joint Communication to the European Parliament, the European Council, the Council, The European Economic and Social Committee and the Committee of the Region,* op. cit.

38 See the website of NATO StratCom COE (https://www.stratcomcoe.org).

39 Wardle and Derakhshan, op. cit.

40 Parliamentary Assembly of the Council of Europe, Resolution 2143 (2017), *Online Media and Journalism: Challenges and Accountability*, http://semantic-pace.net/tools/pdf.aspx?doc=aHRocDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZDoyMzQ1NSZsYW5nPUVO&xsl=aHRocDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTIzNDU1.

CBMs. In practice though, the composition of the OSCE, consisting of states with widely diverging rule of law practices, and with Russia as one of its most prominent members, and its *modus operandi*, heavily dependent on political consensus, make the organization rather powerless.[41]

OSCE documents on international disinformation are few, and they are not always very specific, *but* there are significant exceptions, especially in the sphere of CBMs. A key OSCE document on disinformation is the 2015 'non-paper', brought out together with other international organizations. The paper expresses the ambition to 'facilitate' the member states 'in formulating national and international law and policy' with regard to the spread of 'propaganda' (especially linked with the conflict in Ukraine).[42] In this and other documents,[43] the OSCE approaches disinformation primarily from a domestic human rights perspective (the freedom of information), rather than from an international political one. The OSCE does refer to the international risks of information manipulation, but in very general terms and without blaming individual states. The joint paper expresses the opinion that the dissemination of information which is based on 'vague and ambiguous ideas' is incompatible with international standards on freedom of expression, and that state actors should abstain from doing it.[44] The OSCE and its partner organizations recommend the application of international human rights standards to disinformation, and advocate to include European and international jurisprudence and standards 'to secure the effective exercise of freedom of expression'. The application of these principles and standards are not so much aimed against the international manipulation of information, but against restrictions of media pluralism and

41 Indicative is the exchange of complaints by the United States and Russia missions to the OSCE on Russia's alleged spread of disinformation in the Western Balkans. (*United States Mission to the OSCE. Response to Russian Disinformation About Interference in Macedonia* (PC.DEL/1422/18/Rev.1. 16 November 2018), https://www.osce.org/permanent-council/403991?download=true).

42 *Propaganda and Freedom of the Media*. OSCE. The Representative on Freedom of the Media. Vienna, 2015, https://www.osce.org/fom/203926?download=true.

43 See also OSCE. The Representative on Freedom of the Media, *International Standards and Comparative National Approaches to Countering Disinformation in the Context of Freedom of the Media,* Vienna, March 2019, https://www.osce.org/representative-on-freedom-of-media/424451?download=true.

44 Special rapporteurs of the Organization of American States, United Nations Human Rights Office of the High Commissioner, OSCE, and the African Commission on Human and Peoples' Rights, *Joint Declaration of Freedom of Expression and 'Fake News,' Disinformation and Propaganda*, FOM.GAL/3/17, 3 March 2017 https://www.osce.org/fom/302796?download=true.

the freedom of expression by predatory governments in individual countries. Disinformation in international relations is essentially reduced to propaganda for war and hatred, which allegedly challenges 'the very foundations of the OSCE principle of comprehensive security in Europe'. In a 2019 document on countering disinformation, the OSCE Representative on Freedom of the Media reiterates the argument. The representative calls upon member states 'to abolish general prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news" or "non-objective information", as '*incompatible with international standards* [emphasis in original]'.[45] Also from 2019 are recommendations by the OSCE High Commissioner on National Minorities on refraining from disinformation specifically with regard to national or ethnic minorities. This is especially relevant because minorities' issue are often at stake in disinformation efforts.[46]

There is much to be said for the emphasis that the OSCE and other international organizations put on the freedom of information and expression as key principles in the counter-disinformation effort. It is far from obvious that the principle of the freedom of expression always takes precedence over protection against (foreign) disinformation. The aim for democratic governments remains to fight disinformation without unduly limiting essential freedoms. A recent report commissioned by the European Parliament expressed exactly this challenge, arguing that the restrictive measures against disinformation content 'may pose a greater harm to democracy than disinformation itself'.[47] The answer is a proportional, liberal, participatory and context-specific response to disinformation.[48] But again, there is no one-size-fits-all approach. Counteracting interference in presidential elections in the United States or France or disinformation campaigns in Germany and the Netherlands demands a different response from resisting Russia's intervention in its neighbouring countries, which have a weaker democratic infrastructure, are in a more vulnerable position towards Russia, and which often house significant Russian-language minorities ('compatriots' in the Kremlin-jargon), who prefer to consume Russian state-controlled media.

45 OSCE. The Representative on Freedom of the Media, *International Standards and Comparative National Approaches*, op. cit.

46 OSCE, High Commissioner on National Minorities, *The Tallin Guidelines on National Minorities and the Media in the Digital Age & Explanatory Note.* The Hague, February 2019, https://www.osce.org/hcnm/tallinn-guidelines?download=true.

47 *Disinformation and Propaganda*, op. cit.

48 Jeangène Vilmer, op. cit., p. 13

5 Is Disinformation a Security Issue?

How relevant is disinformation among states? Is disinformation a security issue? A simple reference to history does not suffice. True, disinformation is of all times. States, ruling elites and their servants have always engaged in activities to confuse, divide, attract and engage other peoples in order to increase their own power and influence. However, the historical analogy works only to a certain extent. The intentions of foreign actors may not have changed fundamentally, but the means at their disposal have. The essential novel, and potentially most threatening aspect of disinformation today is its rapidly developing technology, in combination with the large number of potential users. Technology defines the unprecedented breadth, width and depth of disinformation. It makes disinformation much faster, much more sophisticated, and much more difficult to distinguish from information that has no intention to mislead. The number of (potential) users and initiators of disinformation has grown massively. It gives an unprecedentedly 'popular' dimension to what has always been an elitist political game, foreign policy and the relations among states.

In the context of security, disinformation can have domestic and international repercussions. It potentially affects the stability of the domestic order as well as international relations. The allegedly disruptive effect of disinformation on the institutions and procedures of democracy has attracted most attention, its international effects less so. During the first three years of its existence, the EU Task Force asserts to have detected, catalogued and analysed over 4,500 cases of disinformation from the Russian Federation.[49] The figures are impressive, but the effects remain uncertain. Effectiveness concerns impact, which implies causation, or the credible linkage between disinformation, political behaviour and political outcome. This is more easily assumed than it can be proven. There is no evidence that disinformation campaigns have critically influenced the outcome of elections.[50] It is impossible to argue with certainty that Donald Trump would not have been elected or that the Brexit vote would not have been won without Russian interference. It is near impossible to isolate the effect of external interference from the domestic influences that seek the same effect.

The opposite claim, that international disinformation has no or little real political impact, seems equally flawed. Still, in the field of international disinformation it is easier to demonstrate failure than success. If one can reasonably

49 European Commission, 5.12.2018. JOIN(2018), op. cit.

50 See also A. Shekhovtsov, *Russian Interference, And Where to Find It*, European Platform for Democratic Elections, Berlin, n.d., EPDE_bookA5_Rusinterf_EN_DO2.pdf.

assert that foreign state actors were engaged in the manipulation of information, one can then compare these actors' preferences with the actual political outcome. This should give a clear indication of how successful the foreign disinformation strategy was. The election of Emmanuel Macron as president of France serves as an example. The Kremlin did little to hide that Marine le Pen was its favourite candidate, after the conservative François Fillon had decided to leave the race. The defeat of Le Pen and the election of Macron indicate that in this specific instance, Russia's digital creativities did not have the desired political effect.

The potential influence of disinformation largely depends on its level of sophistication and on the context in which it is used. New technologies create new opportunities. Developments in audio and video seem particularly challenging. Deep-fakes, including deep-fakes of real-time news items, have the potential to ignite great trouble. Before anyone even had the time to expose their fallaciousness, deep-fakes may have already ignited major disturbances. The hypothetical examples given in a recent piece on 'post-truth geopolitics'[51] appear alarmingly real: possible fake videos that show an American general in Afghanistan burning a Koran, an Israeli prime-minister contemplating an attack on Iran, or a French president covertly admitting corruption. The possibilities are endless; the consequences are uncertain. Context seems particularly important though. No country, no society is impervious to the political consequences of disinformation. But the level of vulnerability differs, depending on domestic circumstances. Polarized societies are more susceptible to political manipulation of information than less divided ones. Foreign disinformation may have a greater impact on elections in winner-take-all electoral systems than in multi-party ones where government rests on coalition-building. Countries that host significant minority diasporas are more vulnerable to interference by foreign states than more homogeneous countries.

Disinformation seems at most a soft security challenge.[52] The domestic and international effects of disinformation are causally related. Misleading, confusing and dividing the population in other countries may be an objective in and of itself, but for disinformation to have serious international consequences, manipulated ideas among significant parts of the population need to be translated into state policies, which reflect the foreign policy ambitions of the

51 R. Chesney and D. Citron, 'Deepfake and the New Disinformation War: The Coming Age of Post-Truth Geopolitics', in *Foreign Affairs*, January / February 2019, pp. 147–155.

52 I refer to disinformation only, not to other cyber-related activities, including cyber-attacks, stealing information and related criminal acts, or cyber-activities in the military sphere.

disinforming state. It is not impossible. Brexit is a political event of great strategic importance. It undermines the global position of the European Union; it favours its competitors. Brexit has strategic effects, in terms of international alignment and balance of power. The point however is that there is no compelling evidence that the Brexit vote was decisively manipulated from abroad.

To the extent that it can be reasonably assumed, information manipulation did not have a fundamental impact on foreign policies by 'disinformed' governments. As in domestic politics, disinformation in international relations parasites on existing divisions and concerns. Information manipulation has not created these differences, it exploits them. This should not be trivialized. It is disruptive and it further deteriorates the overall international sphere. But it is not a significant security challenge per se, and it does not change the international power balance.

6 Conclusion: CBMs and International Disinformation

Even though the strategic effects of disinformation may have been 'exaggerated',[53] there is ample reason to take the international manipulation of information seriously, and to try to counter it. The effect of disinformation cannot be measured (only) by the extent to which it reaches its ultimate aim, the disinforming country's strategic position.

Practically all counter-measures proposed or taken by European governments and international organizations focus on the protection and resilience against disinformation, and not so much on ways how to deal with its underlying causes, whether within or between states. There is no meaningful discourse on international talks, negotiations, agreements, or CBMs in the field of disinformation; discussions that do exist in the sphere of cyber conflict more generally. The European Parliament explicitly criticized Russia for 'exploiting the absence of a legal international framework in areas such as cybersecurity and the lack of accountability in media regulation',[54] but as yet, it has not been able to develop any meaningful initiatives of its own. Paradoxically, perhaps ironically, it was Russia that in February 2019 asked the OSCE Office of the Representative on Freedom of the Media to provide a comparative analysis

53 A. Lanoszka, 'Disinformation in International Politics', in *European Journal of International Security*, April 2019, 1 (DOI: 10.1017/eis.2019.6).

54 European Parliament, *EU Strategic Communication to Counteract Anti-EU Propaganda by Third Parties*, 23 November 2016 (2016/2030(INI)), http://www.europarl.europa.eu/doceo/document/A-8-2016-0290_EN.pdf.

of 'legislative norms and practices in the sphere of countering the spread of false information', in order to feed further discussion on the issue among the OSCE member states.[55] In its doctrine on information security Russia deplores the absence of international legal norms that may regulate relations between states in the information sphere. It is part of the reason, as the doctrine formulates it, why it proves so difficult to build an 'international information security system' which protects states' (including Russia's) information sovereignty and helps to create strategic stability.[56]

It is difficult to start a meaningful discourse on the international manipulation of information, as long as no state admits to be engaged in disinformation. CBMs were introduced when adversaries continued to disagree and to distrust each other, but also recognized the need to limit the potential for conflict and escalation. The 'exemplar', the bench-mark for all subsequent CBMs was the Final Act of the Conference on Security and Co-operation in Europe, Helsinki, Finland.[57] However, CBMs in the sphere of international information seem far more challenging than in the field of military security. The difficulties to define the parameters of disinformation, the speed of technological developments, and the need to involve relevant non-state actors, including powerful private firms as Facebook, Google and Twitter, makes the CBM's effort unprecedentedly complex. That is no reason though not to exploit the possibilities, and international governmental organizations like the OSCE could take further initiatives.

In the field of disinformation, or in the cyber domain generally, it seems naïve, if not dangerous, to rely on technological solutions only. Technology is part of the answer, not *the* answer. Principally, disinformation is a *political* issue. The most effective way to deal with disinformation is to eliminate the deeper tensions and divisions in societies that it aims to exploit. This is a herculean task though, that goes far beyond the issue of disinformation only. The same goes for disinformation as a foreign policy goal. It asks for political countermeasures. The technology is here to stay, and so is the competition between states. If we take these for granted, there are few other options but to focus on mitigating political strategies, including the elaboration of CBMs.

Interestingly, already in 2013, before disinformation became the hot issue which it is today, the Permanent Council of the OSCE agreed on a decision to step up efforts to address the international security dimensions of the use of

55 OSCE. The Representative on Freedom of the Media, *International Standards and Comparative National Approaches*, op. cit.

56 *Doktrina Informatsionnoi Bezopasnosti Rossiiskoi Federatsii*, op. cit.

57 E.D. Borghard and S.W. Lonergan, 'Confidence Building Measures for the Cyber Domain', in *Strategic Studies Quarterly*, Fall 2018, pp. 10–49.

information and communication technologies (the notion of 'disinformation' was not mentioned). It also decided to work on a range of voluntary CBMs to enhance understanding and cooperation, and to reduce the risk of conflict. The eleven measures focused on a common understanding of key concepts and definitions, through the exchange of national views and terminology related to information and communication technology and its potential threat to international stability. States should work towards a commitment to consult and cooperate in order to reduce the risk of misperception and to facilitate communication and dialogue. And finally, member states agreed on the OSCE becoming the principal hub of the confidence-building effort.[58] In 2016 the Permanent Council of the OSCE revisited the issue. The Council reiterated the CBMs that were first adopted in December 2013, and added five additional ones.[59] Given that the international environment had meanwhile drastically deteriorated, partially also because of alleged international disinformation campaigns by Russia, the lack of any meaningful progress is perhaps less remarkable than the fact that the Council discussed the issue at all again.

The dialogue on CBMs in the information sphere is still in its infant stage. The focus is on defining the issue, exchanging ideas, on first steps towards consultation and possible cooperation. Follow-up measures which may eventually lead to normative or legal restraints on the behaviour of states are still far away, but they are not inconceivable. Fear of uncertain consequences, reputation costs and domestic pressure as a result of the internalization of international norms may lead states and relevant private businesses to accept restraints on their policies, Joseph S. Nye speculates on international relations in the cyber sphere.[60] There is no reason to believe that these considerations would not also apply to the politics of international information. Throughout history, states and societies have been quite effective in learning to cope with the highly disruptive effects of technology.[61]

58 OSCE Permanent Council, *Decision No. 1106, Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication* Technologies, PC.DEC/1106. 3 December 2013, https://www.osce.org/pc/109168?download=true.

59 OSCE Permanent Council, *Decision No. 1202. OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies.* PC.DEC/1202, 10 March 2016, https://www.osce.org/pc/227281?download=true.

60 J.S. Nye, *Normative Restraints on Cyber Conflict,* Harvard Kennedy School / Belfer Center for Science and International Affairs, Cambridge Mass., August 2018, https://www.belfercenter.org/sites/default/files/files/publication/Nye%20Normative%20Restraints%20Final.pdf.

61 Idem.