



Wilfried  
**Martens Centre**  
for European Studies

# Political Warfare: Competition in the Cyber Era

Antonios Nestoras



## Policy Brief

April 2019

The concept of political warfare is not new. Today, however, with the emergence of cyberspace as the fifth domain of war, the scope of political warfare, its diversity and its level of sophistication signify a break from past experience. What early ideas about political warfare identified as propaganda, psychological operations, or a race for the hearts and minds of the population can now be applied on a scale never seen before. This article offers a new frame of reference for an old problem. In order to assess and adapt to the complex nature of inter-state competition in the cyber era, we need to understand how information technology is raising the relative importance of political warfare by transforming the social environment and its instruments of operation. Furthermore, although information technology is a neutral variable, the openness of Western societies increases the vulnerability of liberal democracies to political warfare. As a result, authoritarian regimes, terrorist groups and other revisionary forces of the twenty-first century are undermining democracy and freedom around the world by targeting the network society and by establishing new, virtual spheres of influence.

**Keywords** Political warfare – Hybrid attacks – Cyber – Disinformation – Fake news – Information technology



# Introduction

---

Information technology and new media have revolutionised the ways we connect and communicate with each other, the ways in which we make transactions and trade, and also the ways we argue, fight and establish superiority over others. The Internet is both a 'global village' where time and distance are irrelevant for its social networks and the free flow of information, and a vast 'virtual battlespace' where state and non-state actors compete for power and influence.<sup>1</sup> Cyberspace is first and foremost a neutral computer network where people and nations interact, communicate and transact, but it is also a sphere of influence and an arena for competition—it is the fifth domain of war.<sup>2</sup>

Competition in cyberspace has developed the characteristics of an ideological conflict and features a range of non-violent or unconventional methods, including disinformation, propaganda and psychological operations. Ideological competition and propaganda have always been around—but they have never been applied on such a massive scale and with this level of technological sophistication. The arrival of the cyber era has amplified the relative importance of unconventional warfare as a component of state strategy, as cyberspace is unrestrained by geographical boundaries and law, and devoid of the etiquette and rituals of conventional armed conflicts.

In this sense, competition in cyberspace has developed into a *political warfare* that is testing the limits of the post-war liberal world order. Authoritarian regimes and revisionist powers show a preference for this type of political warfare and are scrambling for influence online, while new—virtual—spheres of influence are opening up in cyberspace. This is nothing short of a fight over the dominant values and forms of governance that will shape the future world order.

There is a multitude of buzzwords that frame the rising importance of information, networks and competition in cyberspace, including information warfare, psychological operations, disinformation and propaganda, cyberwarfare and hybrid warfare. Despite an implicit consensus that technology is playing a major role in changing the operational nature of warfare, no long-term perspective has been developed that considers how information technology—that is, computer

---

<sup>1</sup> M. M. E. Manjikian, 'From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik', *International Studies Quarterly* 54/2 (2010), 381–401.

<sup>2</sup> NATO officially recognised cyberspace as a domain of warfare on 14 June 2016. In 2017, the new US National Security Strategy made reference to the new threats and challenges of the cyber era.



networks and new media—is changing the environment that states operate in and the instruments that they have at their disposal to compete in cyberspace.

This article makes an attempt to offer a new frame of reference for competition in the cyber era, one which is based on the concept of political warfare—a concept broad enough to include other terms and its operational interests, such as propaganda, psychological operations and information warfare. The first section discusses a variety of definitions of political warfare in search of conceptual clarity. The second section engages with the concept of and the literature on the ‘network society’ in order to consider how modern information technology has transformed our societies and, by extension, the operational environment of political warfare. The third section summarises the variety of instruments that states and other international actors have at their disposal. The fourth section introduces the concept of ‘virtual spheres of influence’ in order to discuss the practical effects of political warfare in the cyber era. Implications for the EU, followed by a set of recommendations for countering political warfare, are discussed in the fifth and final section.

## Political warfare: old and new definitions

---

The term ‘political warfare’ goes as back as far as the Second World War. In 1942, the Political Warfare Executive of the British Government compiled a brief but broad-ranging manual titled, *The Meaning, Techniques and Methods of Political Warfare*. The manual understood political warfare as an ‘indispensable component of Total War’ and made a distinction between ‘publicity’ as the broadcasting of information and ‘propaganda’ as the dissemination of misleading information. It described political warfare as a ‘systematic process’ that employs both publicity and propaganda in order to ‘influence the will and so direct the *actions* of peoples in enemy and enemy-occupied territories, according to the needs of higher strategy’.<sup>3</sup> At that time, the British Government identified several instruments of political warfare, including radio broadcasts, leaflets and whispers; the reconditioning of prisoners of war; front-line propaganda spread via loudspeakers and the aerial dissemination of leaflets; the handling of the press and the taking over of radio stations during the reoccupation of enemy-held ter-

---

<sup>3</sup> Emphasis in the original. UK, Political Warfare Executive, *The Meaning, Techniques and Methods of Political Warfare*, British National Archives (1942), FO 898/101, 1, 4 and 11.



ritories; and the use of ideas and narratives that meet the fundamental needs of the population for security, dignity and freedom.<sup>4</sup>

Arguably, when the British introduced the term ‘political warfare’ they were fighting a war against rifles, tanks and V-bombs. But they were also fighting against the appeal of the new order and ‘the need for a general political regeneration along Nazi lines in Europe’;<sup>5</sup> against Hitler sympathisers and American neutrality;<sup>6</sup> and against the proliferation of satellite states, collaborationist movements and Hitler’s copycats in several European countries.

However, even after the war, in the US, George F. Kennan used the same terminology. In a 1948 policy memorandum on the problem of the ‘inauguration of organised political warfare’, Kennan introduced a much broader definition, writing that ‘political warfare is the employment of all the means at a nation’s command, short of war, to achieve its national objectives.’<sup>7</sup>

Still, one could argue that all wars are political and the use of the term ‘warfare’ should be limited to ‘the physical conduct of war or the fighting and violent aspects of war’.<sup>8</sup> However, it is clear from the above that neither the American nor British views of political warfare referred to the state of armed conflict, where kinetic force is applied and physical harm is caused, but to a state of competition or open hostility that is carried on with non-violent tools, overt and covert, such as public diplomacy and propaganda, terror and psychological warfare, and a whole range of methods and techniques that deal with the control and manipulation of information. Hence, the term ‘political’ is used to exclude the violent aspects of war; and the term ‘warfare’ is not an oxymoron, because it can still refer to a particular condition of competition or hostility in the absence of military conflict.

---

<sup>4</sup> Ibid., 5–10.

<sup>5</sup> See A. J. Toynbee, *Survey of International Affairs: 1939–1946: Hitler’s Europe* (London: Oxford University Press, 1954), 118.

<sup>6</sup> For Nazi influence in the US see, for example, B. W. Hart, *Hitler’s American Friends: The Third Reich’s Supporters in the United States* (New York: Thomas Dunne Books, 2018); and S. J. Ross, *Hitler in Los Angeles: How Jews Foiled Nazi Plots Against Hollywood and America* (New York: Bloomsbury, 2017); see also N. J. Cull, *Selling War: The British Propaganda Campaign Against American ‘Neutrality’ in World War II* (New York: Oxford University Press, 1997).

<sup>7</sup> G. F. Kennan, *On Organizing Political Warfare*, US History and Public Policy Program Digital Archive, Redacted Document 269, FRUS, 30 April 1948.

<sup>8</sup> F. Hoffman, ‘On Not-So-New Warfare: Political Warfare vs. Hybrid Threats’, *War on the Rocks*, 28 July 2014.



This understanding seems to be the case with more recent uses of the term ‘political warfare’,<sup>9</sup> which have coincided with the appearance of a variety of overlapping terms, such as ‘information warfare’, ‘psychological operations’, ‘cyberwarfare’, ‘hybrid warfare’ and even ‘neuro-warfare’, each of which claims its own space and relevance.<sup>10</sup> The term that is closest to ‘political warfare’ and deserves closer inspection is ‘hybrid warfare’, which in general involves a similar conceptualisation, whereby the belligerent uses a mix of irregular tactics, such as propaganda, guerrilla warfare and insurgency, in conjunction with the conventional application of kinetic force.<sup>11</sup> Before we go any further it is necessary to attempt a brief disambiguation of hybrid warfare in relation to political warfare.

András Rácz has described hybrid war as a new generation of warfare, employing ‘the combined use of military and non-military means . . . basically the whole spectrum of a state’s policy inventory, including diplomatic, economic, political, social, information and also military means’.<sup>12</sup> The US military has identified a hybrid threat as ‘any adversary that simultaneously and adaptively employs a tailored mix of conventional, irregular, terrorism and criminal means or activities in the operational battlespace’.<sup>13</sup>

For the term ‘hybrid’ to apply, the use of conventional types of warfare is absolutely necessary. This necessity is a rather limiting factor in the application of the term, because in most cases, the mobilisation of the army never happens. Most

---

<sup>9</sup> See, for example, P. A. Smith, *On Political War* (Washington, DC: National Defense University Press, 1989); F. R. Barnett and C. Lord (eds.) *Political Warfare and Psychological Operations: Rethinking the US Approach* (Washington, DC: National Defense University Press, 1989); M. Boot and M. Doran, ‘Political Warfare’, Council on Foreign Relations (28 June 2013); S. G. Jones, *The Return of Political Warfare*, Center for Strategic and International Studies (2 February 2018); R. S. Cohen, ‘Political Warfare is Back with a Vengeance’, *The National Interest*, 12 April 2018; M. Noonan, ‘Re-Inventing Political Warfare’, *US News & World Report*, 16 August 2013; L. Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica: RAND Corporation, 2018); A. Polyakova and S. P. Boyer, *The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition*, Brookings (Washington, DC, March 2018).

<sup>10</sup> For information warfare, see M. C. Libicki, *What is Information Warfare?*, Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University (Washington, DC, 1995); for psychological operations see, for example, M. Taillard and H. Giscoppa, *Psychology and Modern Warfare: Idea Management in Conflict and Competition* (Basingstoke: Palgrave Macmillan, 2013); for cyberwarfare see, for example, R. A. Clarke and R. K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2012); and for neuro-warfare see A. Krishnan, *Military Neuroscience and the Coming Age of Neurowarfare* (London: Routledge, 2017).

<sup>11</sup> For examples of the literature on Russian hybrid warfare, see O. Friedman, *Russian ‘Hybrid Warfare’: Resurgence and Politicization* (London: Hurst, 2018); A. Lanoszka, ‘Russian Hybrid Warfare and Extended Deterrence in Eastern Europe’, *International Affairs* 92/1 (2016), 175–95; A. Rácz, *Russia’s Hybrid War in Ukraine: Breaking the Enemy’s Ability to Resist*, Finnish Institute of International Affairs (Helsinki, 2015).

<sup>12</sup> Rácz, *Russia’s Hybrid War in Ukraine*, 87.

<sup>13</sup> Cited in R. W. Glenn, ‘Thoughts on “Hybrid” Conflict’, *Small Wars Journal*, 2 March 2009.



of the time, what we are left with is just the application of diplomatic, economic, political and social means and a range of influence-gaining tactics, especially in cyberspace. Indeed, Russia's conduct in Ukraine may have been a textbook case of hybrid war, but the non-military elements of this war are part of everyday Russian foreign policy.<sup>14</sup> Rácz admits that in what he calls the 'preparatory phase of Hybrid Warfare'—that is, before the mobilisation of the armed forces—it 'is practically impossible to determine whether . . . influence-gaining measures may be serving as preparation for a hybrid attack'.<sup>15</sup>

Hybrid warfare is a rare combination of non-conventional tools of influence and the use of military force. Most of the time, before the troops are mobilised (if they ever are), the states involved wage political war as they scramble to win the hearts and minds of the people and compete for popularity in cyberspace. The 'preparatory phase' of hybrid warfare might just be the canon—the new normal—in international affairs. And this is why the term 'political warfare' may be more useful in framing the new inter-state or network competition in cyberspace.

Hybrid threats are conceivable, and one should be prepared to face and counter them.<sup>16</sup> However, too much focus on hybrid threats may divert our attention away from the ever-present threat of political warfare. Influence-gaining actions should always be considered as having the potential to escalate into hybrid conflict, but before war turns hybrid, it is purely political.

## Political warfare, information technology and the network society

In *Warrior Geeks*, Christopher Coker examines how technology is transforming the way we fight and think about war in the twenty-first century. Coker's claim is that humans and technology have co-evolved and will continue to do so. So, if war is a 'human thing', as Thucydides said, the most pervasive of social experiences and inherent in human nature, then war is constantly adapting to evolving human technology. Coker's rather pessimistic conclusion is that modern technologies

<sup>14</sup> Rácz, *Russia's Hybrid War in Ukraine*, 58.

<sup>15</sup> *Ibid.*, 59.

<sup>16</sup> In this regard, the establishment of the European Centre of Excellence for Countering Hybrid Threats is a move in the right direction.



can make war a ‘post-human thing’, an even more brutal business that grows out of the pages of cyberpunk dystopias.<sup>17</sup> Technology is also driving the revolution in military affairs (or RMA), having a tremendous impact on military equipment and, consequently, on the way that armies wage war.<sup>18</sup> In fact, the cyber era is having an overwhelming effect on every dimension of power and strategy.<sup>19</sup>

Although Coker’s warnings about post-human war refer to the introduction of artificial intelligence and robotics—not information technology—and RMA refers strictly to military equipment and operational complexities, the point is still that technology is changing the way humans wage war. Political warfare also seems to be adapting to information technology like other modes of competition and conflict. Information technology, that is, computer networks and new media, is expanding both the environment in which political warfare operates and the range of actions that states and other actors have at their disposal.

In the cyber era, the objective reality and the essential features of the individual, of social groups and, ultimately, of the society as a whole, differ radically from how they were understood in previous decades when British and American executives invoked the concept of political warfare. While the information technology that underpins the Internet relies on computer networks, simultaneously and inevitably, society itself is becoming more networked.

In *The Rise of the Network Society*, Manuel Castells claims that just as the Industrial Revolution completely changed the world in the eighteenth and nineteenth centuries, the information revolution that started in the 1970s has activated new modes of economic production, new social formations and a distinctive global culture.<sup>20</sup> According to him, on a more profound, philosophical level, this global transformation is due to the collapse of our traditional concepts of space and time. What this means is that the new technological paradigm—instant communication, social networks and uninterrupted flows of information—has flattened geographical distances, political borders, and the time and effort it takes for information to traverse them. This ‘timeless time’ and ‘space of flows’, as Castells calls them, are

---

<sup>17</sup> C. Coker, *Warrior Geeks: How 21<sup>st</sup>-Century Technology is Changing the Way We Fight and Think About War* (New York: Columbia University Press 2013), xiii.

<sup>18</sup> For literature on RMA, start with J. Hazlett and M. C. Libicki, *The Revolution in Military Affairs* (Washington, DC: Institute for National Strategic Studies, 1994); for something more recent with a focus on the wider consequences of information technology for war and strategy, see J. Henrotin, *The Art of War in the Network Age: Back to the Future* (London: ISTE Ltd.; Hoboken, NJ: Wiley, 2016).

<sup>19</sup> J. Arquilla and D. F. Ronfeldt (eds.), *In Athena’s Camp: Preparing for Conflict in the Information Age* (Santa Monica: RAND Corporation, 1997).

<sup>20</sup> M. Castells, *The Rise of the Network Society* (Malden, MA: Blackwell Publishers, 1996, 2<sup>nd</sup> edn.).





the new material foundations of a very 'real virtuality'.<sup>21</sup> Cyberspace is a virtual space. However, it is not an abstract ethereal domain, but a material one—societies, nations and individuals all share an objective reality there.

Jan van Dijk called computer networks the 'nervous system' of the network society and the infrastructure of cyberspace. Technology has created an information intensive society with a 'culture dominated by media and information products with their signs, symbols and meanings'.<sup>22</sup> The network society is 'a social formation with an infrastructure of social and media networks enabling its prime mode of organization at all levels'.<sup>23</sup>

Network theory and network analysis have come a long way since the 1990s—when both Castells and van Dijk published their seminal works—and now provide some key methodological frameworks for a range of social sciences, from communications studies to sociology. In international relations, engagement with network theory and analysis has been less spectacular; nevertheless, despite many methodological issues, the view of the international system as a network of actors (individual states, intergovernmental organisations, etc.) has already challenged conventional ideas in the field about the concept of power.<sup>24</sup>

If networks are groups or systems where interconnected actors exchange information and resources, then the position of an actor in a network can also be a source of power to influence the behaviour, identity and interests of other actors.<sup>25</sup> Power, therefore, is no longer derived solely or even primarily from individual attributes, such as material capabilities. A central position in the network may also facilitate collective coercive behaviours at the expense of more peripheral and less connected actors.<sup>26</sup> In some cases, the exploitation of an actor's network

---

<sup>21</sup> Ibid., 403, 407 and 460.

<sup>22</sup> J. van Dijk, *The Network Society: Social Aspects of New Media* (London: Sage, 2006), 19.

<sup>23</sup> Ibid., 20.

<sup>24</sup> E. M. Hafner-Burton et al., 'Network Analysis for International Relations', *International Organization* 63/3 (2009), 574.

<sup>25</sup> D. Knoke, *Political Networks: The Structural Perspective*, *Structural Analysis in the Social Sciences* (Cambridge: Cambridge University Press, 1990), 9; L. C. Freeman, 'Centrality in Social Networks: Conceptual Clarification', *Social Networks* 1/3 (1979), 215–39; K. S. Cook et al., 'The Distribution of Power in Exchange Networks: Theory and Experimental Results', *American Journal of Sociology* 89/2 (1983), 275–305.

<sup>26</sup> E. M. Hafner-Burton and A. H. Montgomery, 'Power Positions: International Organizations, Social Networks, and Conflict', *Journal of Conflict Resolution* 50/1 (2006), 11. For a similar argument expressed in the terms of world polity theory, see J. Beckfield, 'Inequality in the World Polity: The Structure of International Organization', *American Sociological Review* 68/3 (2003), 401–24.





position in order to gain social power may even counterbalance the actor's deficiency in other forms of power, for example, economic and military capabilities.<sup>27</sup>

With this in mind, we can put political warfare into perspective if we consider public opinion itself as a network structure. Conceivably, the privileged position of a state in the public opinion of the network society can be a legitimate source of power that enables the state to set the agenda, establish norms and raise support, much as it allows a state to initiate a militarised dispute, frame a conflict or apply pressure to states in less privileged positions.

Once considered as too volatile, incoherent and of no consequence for foreign policy, public opinion boosted by mass media is today understood as a potent actor in foreign affairs.<sup>28</sup> In the age of massive computer networks, breaking news and social media, the whole range of international relations depends, as never before, on real-time popular consent. The network society interacts with every inch of foreign policy and the full range of national objectives, from membership of international organisations to the choice of friends and foes, and, of course, to the decision to go to war.

The 'network society' refers to the new complex patterns of human interaction, information sharing and decision-making in the cyber era. It refers to a society that depends on networks. But it also refers to a society that is highly interactive, meaning that there is a two-way flow of information between the state and the society, influencing each other in new and greatly magnified ways. It would not be an exaggeration to claim that the opinion of the network society on domestic and international affairs is more present and more important than ever.

In this respect, information technology is the capstone to a prolonged shift to total war that started with the Industrial Revolution. After the Great War, conflict was no longer a matter for the few, decided by an elite and fought by an army of professional soldiers or mercenaries.<sup>29</sup> War involved the entire state's infrastructure

---

<sup>27</sup> E. M. Hafner-Burton and A. H. Montgomery, 'Globalization and the Social Power Politics of International Economic Networks', in M. Kahler (ed.), *Networked Politics: Agency, Power, and Governance* (Ithaca, NY: Cornell University Press, 2009), 23–42.

<sup>28</sup> For a pivotal article that changed our perceptions of public opinion in foreign policy decision-making, see O. R. Holsti, 'Public Opinion and Foreign Policy: Challenges to the Almond-Lippmann Consensus, Mer-shon Series: Research Programs and Debates', *International Studies Quarterly* 36/4 (1992), 439–66; more recently by the same author, O. R. Holsti, *Public Opinion and American Foreign Policy* (Ann Arbor: University of Michigan Press, 2004). On the importance of mass media in the interaction between public opinion and foreign policy, see S. Soroka, 'Media, Public Opinion, and Foreign Policy', *The Harvard International Journal of Press/Politics* 8/1 (2004), 27–48.

<sup>29</sup> L. Finch, 'Psychological Propaganda: The War of Ideas on Ideas During the First Half of the Twentieth Century', *Armed Forces & Society* 26/3 (2001), 367–86.



and resources, the masses and the livelihoods of the whole nation, and therefore the decision to go to war needed the support of the people. The people needed to believe in the *Triumph of the Will*<sup>30</sup> and they needed to know *Why We Fight*.<sup>31</sup> This is why propaganda became an essential tool for mobilising the masses in the fast and furious twentieth century, and why today wars are always ‘wars of choice’ that require a high degree of legitimacy for maximum mobilisation and support from the population.<sup>32</sup>

As the cyber era increases the importance but also the vulnerability of public opinion in the network society, it is also taking political warfare to a whole new level, giving states more options and more potent instruments with which to compete for the hearts and minds of the network society.

## Instruments of political warfare in the cyber era

Control of information is key in the race for the hearts and minds of the network society. What is information? It is facts and figures about the world, but it is also the meaning conveyed or represented by a sequence of stories or events that enables humans to reduce the vastness and the uncertainty of our world. We collect information, reflect on information, and make choices or form opinions based on information. Our world, our own significance and existence acquire meaning based on the information we consume. In other words, information is the primary data of our perception of reality and, therefore, whoever controls the information wields the power to influence opinions and decision-making.

Information is also a resource. It can be mined, online, and it can be exploited. It needs to be secured, because it can be corrupted or stolen. It can be used to improve the chances of the military winning wars and it can be used to influence the decision-making process inside a state through hacking a democratic election or swaying public opinion—the importance of which has risen steeply in the cyber era.

<sup>30</sup> L. Riefenstahl (producer and director), *Triumph des Willens* [Triumph of the will], Motion picture (NSDAP Reichspropagandaleitung Hauptabt, 1935).

<sup>31</sup> F. Capra and A. Litvak (producers and directors), *Why We Fight*, Motion picture series (US War Department, 1942).

<sup>32</sup> T. E. Nissen, *The Weaponization of Social Media*, Royal Danish Defence College (Copenhagen, 2015), 8.



In this regard, for political warfare, information is ammunition. And it has a damaging effect regardless of the absence of physical impact.<sup>33</sup> Political warfare in the cyber era refers to the systematic use of a range of diplomatic, economic and information tools, overt or covert, to achieve national objectives outside the context of conventional armed conflict. Political warfare is waged against the network society and it targets the credibility of political institutions, the integrity of liberal democratic processes and the unity of society at large. What earlier conceptions of political warfare identified as propaganda or psychological operations are now applied on a massive scale, as never seen before. The tools employed include disinformation campaigns, the establishment of cross-border political networks, and the use of strategic narratives or myths.

‘Disinformation’ refers to the intentional use of false information in order to mislead the general public.<sup>34</sup> Disinformation includes the systematic spreading of inaccuracies, fabricated stories, doctored images, and other provocative and divisive content across the full spectrum of social and traditional media. The Islamic State, for instance, uses social media as a platform for its propaganda with the aim of intimidating its enemies, recruiting citizens as terrorists and planting sleeper cells in enemy states.<sup>35</sup> In contrast, Russian disinformation involves state-owned media, such as *Russia Today* and Sputnik; troll factories; and automated social media accounts (bots). The ‘Lisa’ case in Germany in 2016 and the #MacronLeaks campaign in France immediately before the 2017 presidential elections are two examples of the confusion and discord that disinformation can cause in the public opinion of a country.<sup>36</sup>

‘Political networks’ refers to overt or covert links between political parties and prominent individuals with the intention of undermining the political process from within. This kind of subversive political intervention may include financial support, public encouragement, or the official endorsement of radical, extremist or

---

<sup>33</sup> See Boothby’s definition: ‘a weapon is an offensive capability that is applied, or that is intended or designed to be applied, to a military object or enemy combatant. A destructive, damaging or injurious effect of the weapon need not result from physical impact as the offensive capability need not be kinetic’; in W. Boothby, *Conflict Law: The Influence of New Weapons Technology, Human Rights and Emerging Actors* (The Hague: Asser Press & Springer, 2014), 176.

<sup>34</sup> For an introduction to disinformation, see B. Nimmo, *Identifying Disinformation: An ABC*, Institute for European Studies, Issue 2016/1 (Brussels, 2016).

<sup>35</sup> For more on the process by which the Islamic State disseminates propaganda through social media, see J. Shaheen, *Network of Terror: How DAESH Uses Adaptive Social Networks to Spread Its Message*, NATO Stratcom Center of Excellence (Riga, 2015). For how the Islamic State uses information operations as a means of intimidation and recruitment, see M. R. Zgryziewicz, *Daesh Information Campaign and Its Influence*, NATO StratCom Centre of Excellence (Riga, 2016); and R. Zgryziewicz, *Daesh Recruitment: How the Group Attracts Supporters*, NATO StratCom Centre of Excellence (Riga, 2018).

<sup>36</sup> S. Meister, ‘The “Lisa Case”: Germany As a Target of Russian Disinformation’, *NATO Review* (2016).



populist forces by the state that is seeking to interfere in the domestic politics of another. For example, the Kremlin has been very active in supporting, funding and feeding disinformation to left- and right-wing populist parties in Europe, whereas Iran has consistently supported terrorist groups in Lebanon and Yemen, among others.<sup>37</sup>

‘Strategic narratives’ are also used as a power base in the context of political warfare. The advances in information and communication technologies—the Internet, blogs and social media—have revolutionised the way states perceive the international system and how they project power within it to increase their influence. In the cyber era the formation and communication of strategic narratives as methods of persuasion and influence is central to foreign policy. States use strategic narratives in a highly complex media setting to sway target audiences.<sup>38</sup> Strategic narratives fit neatly with Joseph Nye’s familiar ‘soft power’ concept, that is, the ability to exert influence on others by framing the agenda, and persuading and eliciting positive attraction based on resources such as culture, values and diplomacy.<sup>39</sup> But even soft power is not always as benign as it sounds: various people have perceived the principle of cultural attraction through public diplomacy as an overly aggressive means of influence or a ‘soft-war’.<sup>40</sup> However, in the case of Russia’s strategic communication with Europe and the West, soft power has reached unprecedented levels of forcefulness and aggression.<sup>41</sup> Russian narratives are anti-Western and explicitly anti-American, claiming that the result of the US-led liberal order in Europe and the rest of the world is growing insecurity, the end of national sovereignty and the erosion of traditional values as a result of multiculturalism. In contrast, the same narrative promotes Russia as an alternative partner who promises to work alongside fellow European countries to restore their sense of self, defend their values and tackle instability.<sup>42</sup>

Although Russia, Iran and the Islamic State apply very different mixes of methods and tactics in political warfare, the above examples illustrate the various ways in which states and terrorist groups wage political warfare to achieve their objectives. At different times and

---

<sup>37</sup> For Russia, see, for example, P. Krekó and L. Gyóri, *Russia and the European Far Left*, Institute of Statecraft (London, 2016); A. Klapsis, *An Unholy Alliance: The European Far Right and Putin’s Russia*, Wilfried Martens Centre for European Studies (Brussels, 2016); P. Krekó et al., *Europe’s New Pro-Putin Coalition: The Parties of ‘No’*, Institute of Modern Russia and Political Capital Institute (2015).

<sup>38</sup> L. Roselle et al., ‘Strategic Narrative: A New Means to Understand Soft Power’, *Media, War & Conflict* 7/1 (2014), 71–4.

<sup>39</sup> J. S. Nye, *Soft Power: The Means to Success in World Politics* (New York: Public Affairs, 2004).

<sup>40</sup> M. E. Price, *Free Expression, Globalism, and the New Strategic Communication* (New York, NY: Cambridge University Press, 2015), 134–52.

<sup>41</sup> For Russia’s use of ‘soft power’ in Ukraine see V. Hudson, “‘Forced to Friendship’? Russian (Mis-)Understandings of Soft Power and the Implications for Audience Attraction in Ukraine”, *Politics*, 35/3 (2015), 330–46; K. Geers (ed.), *Cyber War in Perspective: Russian Aggression Against Ukraine* (Tallinn: NATO CCD COE Publications, 2015). For the same in the Baltic States see M. Winnerstig (ed.), *Tools of Destabilization: Russian Soft Power and Non-Military Influence in the Baltic States*, Swedish Defence Research Agency (FOI) (2014).

<sup>42</sup> J. Szostek, ‘Defence and Promotion of Desired State Identity in Russia’s Strategic Narrative’, *Geopolitics* 22/3 (2016), 1–23.



in various contexts, the political warfare of authoritarian and revisionist forces manifests as a means of intimidating, manipulating and deceiving the network society in order to destabilise an adversary, to avoid retribution for acts of aggression, or to increase the number of supporters for and influence of such forces.

## Political warfare and virtual spheres of influence

---

In line, it seems, with Winston Churchill's prediction that '[t]he empires of the future are the empires of the mind',<sup>43</sup> since the Second World War, states appear to have resisted their primordial desire to seize territory, even when they emerge victorious from a conflict. This absence of conquest is what Mark Zacher has called the 'territorial integrity norm' and it appears to be a distinctive feature (others call it an 'anomaly') of the post-war world.<sup>44</sup> However, if the acquisition of new territory—and the additional resources or geopolitical advantages that come with it—is not among the primary objectives of political warfare, then what could be the endgame of state competition in cyberspace? The answer may lie with Mary Kaldor's 'new wars' that rarely have territorial ends; their weapons of choice are subversion, destabilisation and disruption.<sup>45</sup>

As Niall Ferguson explores in *The Square and the Tower*, networks can be a major source of disruption because they undermine hierarchical institutions and orders.<sup>46</sup> In the cyber era, this disruption seems to be greatly magnified. Political warfare enhances the capacity of states to affect the character, development and behaviour of network societies and, therefore, is an indispensable element of their power to direct or influence other states. A privileged position in the network, the ability to control information flows and content, and power through influence all matter more in the cyber era.

The collapse of the traditional conceptions of space and time has maximised the porosity of geopolitical borders: information can instantly pierce right through

---

<sup>43</sup> W. Churchill, 'The Gift of a Common Tongue', speech made at Harvard University, 6 September 1943.

<sup>44</sup> M. W. Zacher, 'The Territorial Integrity Norm: International Boundaries and the Use of Force', *International Organization* 55/2 (2001), 215–50. For the 'anomaly' thesis, see D. D. P. Johnson and M. D. Toft, 'Grounds for War: The Evolution of Territorial Conflict', *International Security* 38/3 (2014), 33.

<sup>45</sup> M. Kaldor, *New and Old Wars: Organised Violence in a Global Era* (Cambridge: Polity Press, 2013).

<sup>46</sup> N. Ferguson, *The Square and the Tower: Networks and Power, from the Freemasons to Facebook* (New York: Penguin Press, 2018).



them to reach any population. With all its vastness and intricacy, cyberspace has little room for borders, those venerable social artefacts that emerged over centuries, enclosed sovereign nation states and predestined the anarchical nature of the international system. However, the boundaries of sovereignty in cyberspace are not clearly drawn and this engenders a near-permanent state of political warfare.

In *World Order*, Henry Kissinger reflects on the waning world order as a blend of the concept of sovereignty and the balance of power that originated in Europe with the distinct flavour of American idealism.<sup>47</sup> Kissinger claims that the changing nature of the sovereign state, the political reaction to globalisation and the lack of effective global governance are pulling this liberal world order apart. A clash of rival ideas about international affairs may eventually assemble a new world order, and although this clash may not necessarily trigger a war between major powers, Kissinger thinks that it entails the risk of devolving the international system into ‘spheres of influence identified with particular domestic structures and forms of governance’.<sup>48</sup>

In the age of imperialism, spheres of influence constituted a form of indirect rule.<sup>49</sup> Unlike colonies that were under direct imperial administration, countries falling within a sphere of influence were client states: ruled indirectly by faithful local elites, who were in turn over-ruled by the empire’s seat of power.<sup>50</sup> It took a deplorable amount of destruction to dismantle the Imperial Order, but the concept of the spheres of influence as a ‘semi-formal recognition of special rights’ of the great powers survived the onslaught and continued into the Cold War.<sup>51</sup> The spheres of influence of the superpowers were both a strategic buffer zone and a pivot area in which their ideological confrontation oscillated.

In the cyber era, a massive disinformation campaign that misleads social networks and exerts significant influence on parts of the electorate is, at the very least, a dilution of sovereignty in the receiving state. The virtual spheres of influence do not draw from some special right to meddle in another state’s affairs, but they have the (soft) power to affect domestic politics—‘the ability to entice and attract’ the electorate with recourse to this or that value,

---

<sup>47</sup> H. Kissinger, *World Order: Reflections on the Character of Nations and the Course of History* (New York: Penguin Press, 2014), Kindle e-book.

<sup>48</sup> *Ibid.*, ‘Where do we go from here?’, Paragraph 1.

<sup>49</sup> For a conceptual discussion of direct/indirect rule, see J. Gerring et al., ‘An Institutional Theory of Direct and Indirect Rule’, *World Politics* 63/3 (2011), 377–433.

<sup>50</sup> C. Newbury, *Patrons, Clients, and Empire: Chieftaincy and Over-Rule in Asia, Africa, and the Pacific* (Oxford: Oxford University Press, 2003).

<sup>51</sup> J. Donnelly, ‘Sovereign Inequalities and Hierarchy in Anarchy: American Power and International Society’, *European Journal of International Relations* 12/2 (2006), 153.





narrative or story.<sup>52</sup> What is more, the concept of spheres of influence implies a certain military preponderance over a space, which in turn, makes it quite difficult for others to penetrate that space. In contrast, in cyberspace every space and every network is accessible, constantly contested and penetrated by competing actors and narratives.

Indeed, this competition in cyberspace is developing into a real ideological struggle (even if it is not as intense and as clear-cut as during the Cold War). The Internet has increased the plasticity of individual and national identities and has revitalised the ‘political competitions for regional and strategic dominance’ that had previously been considered as settled in the post–Cold War era.<sup>53</sup> The spread of information technology is making Western societies more networked (whereas authoritarian societies are remaining hierarchical), and networks appear to be easier to penetrate and subvert than hierarchies. The authoritarian and revisionist forces of the twenty-first century, including Putin’s Russia, China’s illiberal state capitalism, Iran’s clerical oligarchy and, of course, Islamic State’s grotesque version of Islamist theocracy are attempting to undermine basic liberties around the world by targeting the network society and by establishing new, virtual spheres of influence.

The devolution of Europe into virtual spheres of influence constitutes a real threat for the continent. Russian disinformation operations have manipulated successive crises—and the EU’s inability to deal with those crises effectively—to increase the Kremlin’s grip on Europe and especially on those Eastern European countries with a history of Russian military presence and influence. Russian information campaigns, tailor-made for each country, have spread fear, anger and resentment, fuelling the spectacular rise of illiberal, populist movements in Europe and threatening to derail the post-war order on the continent.

Although the causes of the populist uprising can be located in Europe’s own failings, Russian political warfare is designed to add oil to the fire of European disintegration. In other words, disinformation does not create divisions out of thin air, but rather looks for existing divisionary issues in the public domain and tries to expand the divide. The resulting segmentation provides fertile ground for the emergence of counter-narratives and rival ideologies—a real war of ideas.

---

<sup>52</sup> J. S. Nye, *The Paradox of American Power: Why the World’s Only Superpower Can’t Go It Alone* (Oxford: Oxford University Press, 2003), Kindle e-book, ‘The American Colossus’, ‘Soft Power’, Paragraph 2. This is of course a twisted version of Nye’s soft power, quoted here deliberately out of context.

<sup>53</sup> N. Shadlow, ‘Welcome to the Competition’, *War on the Rocks*, 26 January 2017.





# Political warfare and pro-Russian populism: implications for the EU

The euro and migration crises, followed by a dramatic decline in public support for the EU, have created the constitutive conditions for the spectacular rise of populist parties in Europe.<sup>54</sup> As populism is a broad church embracing several confessions, these parties' political agendas also represent a variety of issues. Between the euro crisis and the migration crisis, however, the positions of European populists on foreign and security policy have received much less attention.

Studies of the foreign policy attitudes exhibited by populist parties from across the board have indicated that left- and right-wing populists are not only Eurosceptic, but in most cases also tend to be anti-American and openly pro-Russian.<sup>55</sup> This tendency is visible in the radical left movements of the crisis-ridden European south, the illiberal populist parties in the East, and even in Western Europe, where the anti-establishment far right is ringing the Russian bell. In all these cases, populists frequently relay disinformation, fake news and strategic narratives that serve the Russian foreign policy agenda.

The European left, still driven to some extent by its traditional anti-Americanism, is also drawn to Putin's apparent confrontation with the West. The alignment between radical left positions in Europe and foreign policy thinking in Moscow may also be attributed to historical links and Putin's anti-capitalist and anti-globalisation posturing.<sup>56</sup> In those parts of Europe where the left has become irrelevant, such as the post-Communist countries, the right is a better conduit for Russian influence. This affiliation of Europe's right with the Kremlin, which is naturally the most pronounced, represents another expression of neo-conservative ideology and the potential for extreme right-wing values.<sup>57</sup>

Both left-wing and right-wing populist views of Russia seem to converge when serving a shared Eurosceptic agenda.<sup>58</sup> In connection with this point, the pro-Russian mannerisms of

<sup>54</sup> See, for example, European Commission, *Standard Eurobarometer 85, Spring 2016, First Results* (July 2016), 14–16; and B. Stokes, *Euroscepticism Beyond Brexit: Significant Opposition in Key European Countries to an Ever Closer EU*, Pew Research Center (7 June 2016).

<sup>55</sup> R. Balfour et al., *Europe's Troublemakers: The Populist Challenge to Foreign Policy*, European Policy Centre (Brussels, February 2016), 32–5; Klapsis, *An Unholy Alliance*; A. Chryssogelos, *Old Ghosts in New Sheets: European Populist Parties and Foreign Policy*, Centre for European Studies (Brussels, 2011); Krekó and Győri, *Russia and the European Far Left*.

<sup>56</sup> Krekó and Győri, *Russia and the European Far Left*, 7.

<sup>57</sup> Klapsis, *An Unholy Alliance*, 17–21.

<sup>58</sup> Chryssogelos, *Old Ghosts in New Sheets*, 17.



European populists could be casually waved off as a ‘marriage of convenience’,<sup>59</sup> an opportune alliance to counter the ‘ever closer’ EU. Indeed, at the onset of the populist surge, these speculative ideological links may have been little cause for concern, even when considered alongside the few documented personal and financial links between Russia and European populist parties or individuals.<sup>60</sup> It is equally true that despite the alarm sounded by several European politicians, populism has not changed political life in Europe as dramatically as it has, for example, in Latin America. Nevertheless, the populist affiliation with the Kremlin is already moving beyond the personal and the discursive to translate into de facto pro-Russian lobbying in Europe. For example, left- and right-wing populists have been pushing in unison to revoke EU sanctions on Russia following the annexation of Crimea, both on the national and the European levels. Also, Russia, as an alternative strategic ally and a source of funds, figured prominently in the Greek drama that unfolded in 2015. Last but not least, the Brexit ‘watershed moment’—which by itself should be enough to demonstrate the amount of damage populism can inflict on the European project—was also a ‘big win for Russia’s foreign policy’.<sup>61</sup>

In addition to loathing the EU for diluting national sovereignty, the populists believe post-war European integration to be part of a bigger plan—a conspiracy even—led by the US that aims to geopolitically subjugate Europe. For example, according to the French new right, the entire transatlantic security architecture represents an organised attempt to subdue the nations of Europe and strip them of national sovereignty.

Left- and right-wing anti-American and pro-Russian convergence is not limited to the national level. In the Committee on Foreign Affairs of the European Parliament, the populist right invariably accuses the US of the geopolitical subordination of the EU, the subjection of the peoples of Europe and the arrangement of a world government. Meanwhile, the populist left deplors the dependence of Europe on the US and the Euro-Atlantic elites. In essence, the populist worldview depicts the US as an empire with the EU as its puppet, and the Euro-Atlantic elites as the executive branch of a global conspiracy to control the European people.

---

<sup>59</sup> Laruelle, M., *Eurasianism and the European Far Right: Reshaping the Europe–Russia Relationship* (Lanham, MD: Lexington Books, 2015).

<sup>60</sup> C. Mudde, ‘Russia’s Trojan Horse’, *Open Democracy*, 8 December 2014.

<sup>61</sup> J. E. Herbst, ‘Brexit is a Win for Putin’, *Atlantic Council*, 30 June 2016.



Similarly, left- and right-wing populists share a view of Russia as a strategic ally and a valuable trade partner for the EU. They claim that Russia contributes to EU energy security, and therefore that EU–Russia relations should be improved and rivalry should be avoided. More than that, the European Neighbourhood Policy could and should anticipate a convergence between the EU and Eurasian integration. Populists have repeatedly asked the EU to lift or discontinue the sanctions on Russia.

Of course, populist positions on foreign policy and the US are not identical everywhere in Europe. There are meaningful variations on anti-American, pro-Russian and even Eurosceptic positions. However, the frequency with which anti-Western elements appear, as well as the nature of the pro-Russian narratives in populist discourse, are suggestive of a loose political movement, or a pro-Russian bloc, which is increasingly influential, willing and able to dissent.<sup>62</sup>

The Kremlin is, of course, only too kind to oblige such views. The Russian disinformation apparatus seems to be fuelling populist rhetoric throughout Europe with official strategic narratives and fake news. For instance, anti-immigration rhetoric from online media outlets and political parties in Central and Eastern European countries frequently echoes false or misleading stories and narratives originating in Russia. On the theme of the refugee crisis, by sowing fear and resentment, the Russian disinformation campaigns have added another arrow to the quiver of the European far right.

The populist worldview—this claustrophobic blend of illiberal and anti-American tirades—corresponds, in subject and in style, conspicuously with Russian disinformation campaigns and strategic narratives in their confrontation with the US, NATO and the EU.<sup>63</sup> Bearing in mind that the world order is evolving into ‘spheres of influence identified with particular domestic structures and forms of governance’,<sup>64</sup> the resonance of Kremlin narratives with populist parties demarcates a new sphere of Russian influence in Europe based on a radical notion of security and a preference for illiberal democracy. If the architecture of European security after the Second World War was designed to keep Russia out of the continent, then the rising pro-Russian populism within the continent points to a new European order in the making.

What the populists seem to implicitly hope for is a rollback to a continental concert that draws on the nineteenth-century balance of power and allows the return of Russia as a major stakeholder in Europe with legitimate interests and a sphere of influence. The world-

---

<sup>62</sup> Krekó et al., *Europe's New Pro-Putin Coalition*.

<sup>63</sup> D. Spechler, ‘Russian Foreign Policy During the Putin Presidency’, *Problems of Post-Communism* 57/5 (2010), 35–50.

<sup>64</sup> H. Kissinger, ‘Henry Kissinger on the Assembly of a New World Order’, *Wall Street Journal*, 29 August 2014.



view of the pro-Russian bloc is patently incompatible with the post-war order in Europe, because it accommodates Russian revisionism in Europe.

## Policy recommendations

---

- In recent years, the public debate over political warfare and disinformation has intensified in the EU institutions. The Commission has introduced a new action plan against disinformation and the Foreign Affairs Committee of the European Parliament has been keeping an eye on the issue. In practical terms, the European External Action Service StratCom East team and the European Centre of Excellence for Countering Hybrid Threats are commendable initiatives that need to guide further thinking and action on the issue of political warfare. The EU needs to maintain and increase its vigilance regarding this potential threat, which may become a definitive security issue in the near future. In line with the draft recommendation of 22 January 2019 of the Committee on Foreign Affairs to the Council and the high representative of the Union for foreign affairs and security policy/vice-president of the Commission, strategic communication needs to become a matter of high priority for the EU.
- Populism, combined with disinformation and political warfare, is a major threat to freedom and democracy for Europe. Although fake news is old news and there is nothing novel in using deception in foreign policy, we have a lot to learn about how state and non-state actors use modern information and communications technology to influence our network society. The EU needs to foster research in this subject, and also implement more actions that will create links between academics and policymakers and raise awareness of how state and non-state actors conduct political warfare and influence operations in Western Europe. Research needs to pay special attention to the roles of Russia, China and Islamic radicalism.
- Information literacy and critical-thinking skills are long-term and cost-effective responses to disinformation, fake news and political warfare in general. The EU and its member states, as well as regional authorities, need to invest in educational initiatives designed to teach higher-order and critical-thinking skills alongside practical skills such as detecting misinformation and disinformation in various online platforms, identifying fake accounts and trolls, dealing with trolling, tracing doctored images, the



ethics of communicating information on social media and so on. These educational activities need not be purely academic in nature; they could also be introduced in primary and secondary education, adult education and lifelong learning programmes.

- The EU should take full legislative action against disinformation and political warfare, in the style of the US Countering Foreign Propaganda and Disinformation Act that was introduced by Congress on 10 May 2016. (The bill was initially called the Countering Information Warfare Act.) In line with the EU's stated objectives concerning strategic communications, this legislative action should create a legal framework for addressing and responding to disinformation activities by external actors, as well as strengthening the overall media environment in the EU member states and beyond.



# Conclusion

---

Competition in the cyber era makes it difficult to make a clear distinction between war and peacetime. In the absence of armed conflict sanctified by a legal document or public pronouncement produced by an elected or otherwise legitimised state entity, international relations are open to various modes of unconventional strategic competition. After all, war and peace are the two extreme situations of our world. In a sense, total war and (total) peace have been extremely rare. So much so, that they may even be singular spots on the fringes of a vast continuum of international relations, which is dotted with everything in between war and peace: diplomacy and propaganda, proxy wars and revolutions, annexations and invasions, cultural influences, trade wars, economic sanctions and incentives, intergovernmental organisations, non-governmental organisations and so on. Perhaps we should not speak of a 'line' that separates war and peace, but of a huge intervening space of other possibilities.

The concept of political warfare fills this space as a mode of international competition and hostility absent of armed conflict. In this sense, political warfare may complement or substitute war entirely, as well as preceding or succeeding armed conflict. Equally it is an indication that strategic competition is open, that the international order should not be taken for granted and that instead global political instability is on the rise. Popularity and social penetration online—that is, a privileged position in the network society—have reinvented the age-old concept of spheres of influence. This could be simply a transitional phase, but it could also signal a complete rearrangement of the international order.

In this context, the combination of political warfare and network theory frames a topical and exciting research agenda. There is still much to learn about the role of the network society in foreign policy and strategy. We need to map, for instance, how strategic narratives and disinformation are propagated online, how states fight for a privileged position in the network society, and how online popularity translates into influence and power for the state. This may also be the time to revisit the debate about the state as a non-unitary actor and how the relative position of networks can challenge strategic cultures, identity and national interests. We might even need to momentarily stop thinking about the state per se and start thinking about domestic and foreign networks that fight using purely political warfare for control of the state in this new, interactive international system of the cyber era.



# Bibliography

Arquilla, J. and Ronfeldt, D. F., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica: RAND Corporation, 1997).

Balfour, R. et al., *Europe's Troublemakers: The Populist Challenge to Foreign Policy*, European Policy Centre (Brussels, February 2016).

Beckfield, J., 'Inequality in the World Polity: The Structure of International Organization', *American Sociological Review* 68/3 (2003), 401–24.

Boot, M. and Doran, M., 'Political Warfare', Council on Foreign Relations (28 June 2013).

Boothby, W., *Conflict Law: The Influence of New Weapons Technology, Human Rights and Emerging Actors* (The Hague: Asser Press & Springer, 2014).

Capra, F. and Litvak, A. (producers and directors), *Why We Fight*, Motion picture series (US War Department, 1942).

Castells, M., *The Rise of the Network Society* (Malden, MA: Blackwell Publishers, 1996, 2<sup>nd</sup> edn.).

Chryssogelos, A., *Old Ghosts in New Sheets: European Populist Parties and Foreign Policy*, Centre for European Studies (Brussels, 2011).

Churchill, W., 'The Gift of a Common Tongue', speech at Harvard University, 6 September 1943, accessed at <https://winstonchurchill.org/resources/speeches/1941-1945-war-leader/the-price-of-greatness-is-responsibility/> on 22 March 2019.

Clarke, R. A. and Knake, R. K., *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2012).

Cohen, R. S., 'Political Warfare Is Back with a Vengeance', *The National Interest*, 12 April 2018, accessed at <https://nationalinterest.org/feature/political-warfare-back-vengeance-25352> on 9 October 2018.

Coker, C., *Warrior Geeks: How 21<sup>st</sup>-Century Technology is Changing the Way We Fight and Think About War* (New York: Columbia University Press, 2013).

Cook, K. S. et al., 'The Distribution of Power in Exchange Networks: Theory and Experimental Results', *American Journal of Sociology* 89/2 (1983), 275–305.





Cull, N. J., *Selling War: The British Propaganda Campaign Against American 'Neutrality' in World War II* (New York: Oxford University Press, 1997).

Dijk, J., *The Network Society: Social Aspects of New Media* (London: Sage, 2006).

Donnelly, J., 'Sovereign Inequalities and Hierarchy in Anarchy: American Power and International Society', *European Journal of International Relations* 12/2 (2006), 139–70.

European Commission, *Standard Eurobarometer 85, Spring 2016, First Results* (July 2016), 14–16.

Ferguson, N., *The Square and the Tower: Networks and Power, from the Freemasons to Facebook* (New York: Penguin Press, 2018).

Finch, L., 'Psychological Propaganda: The War of Ideas on Ideas During the First Half of the Twentieth Century', *Armed Forces & Society* 26/3 (2001), 367–86.

Freeman, L. C., 'Centrality in Social Networks: Conceptual Clarification', *Social Networks* 1/3 (1979), 215–39.

Friedman, O., *Russian 'Hybrid Warfare': Resurgence and Politicization* (London: Hurst, 2018).

Geers, K. (ed.), *Cyber War in Perspective: Russian Aggression Against Ukraine* (Tallinn: NATO CCD COE Publications, 2015).

Gerring, J., et al., 'An Institutional Theory of Direct and Indirect Rule', *World Politics* 63/3 (2011), 377–433.

Glenn, R. W., 'Thoughts on "Hybrid" Conflict', *Small Wars Journal*, 2 March 2009, accessed at <http://smallwarsjournal.com/mag/docs-temp/188-glenn.pdf> on 21 February 2019.

Hafner-Burton, E. M., Kahler, M. and Montgomery, A. H., 'Network Analysis for International Relations', *International Organization* 63/3 (2009), 559–92.

Hafner-Burton, E. M., and Montgomery, A. H., 'Power Positions: International Organizations, Social Networks, and Conflict', *Journal of Conflict Resolution* 50/1 (2006), 3–27.

Hafner-Burton, E. M. and Montgomery, A. H., 'Globalization and the Social Power Politics of International Economic Networks', in M. Kahler (ed.), *Networked Politics: Agency, Power, and Governance* (Ithaca: Cornell University Press, 2009), 23–42.



Hart, B. W., *Hitler's American friends: The Third Reich's Supporters in the United States* (New York: Thomas Dunne Books, 2018).

Hazlett, J. and Libicki, M. C., *The Revolution in Military Affairs* (Washington, DC: Institute for National Strategic Studies, 1994).

Henrotin, J., *The Art of War in the Network Age: Back to the Future* (London: ISTE Ltd.; Hoboken, NJ: Wiley, 2016).

Herbst, J. E., 'Brexit is a Win for Putin', *Atlantic Council*, 30 June 2016.

Hoffman, F., 'On Not-So-New Warfare: Political Warfare vs. Hybrid Threats', *War on the Rocks*, 28 July 2014, accessed at <https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/> on 22 March 2019.

Holsti, O. R., *Public Opinion and American Foreign Policy* (Ann Arbor: University of Michigan Press, 2004).

Holsti, O. R., 'Public Opinion and Foreign Policy: Challenges to the Almond-Lippmann Consensus, Mershon Series: Research Programs and Debates', *International Studies Quarterly* 36/4 (1992), 439–66.

Hudson, V., "Forced to Friendship?" Russian (Mis-)Understandings of Soft Power and the Implications for Audience Attraction in Ukraine', *Politics* 35/3 (2015), 330–46.

Johnson, D. D. P. and Toft, M. D., 'Grounds for War: The Evolution of Territorial Conflict', *International Security* 38/3 (2014), 7–38.

Jones, S. G., *The Return of Political Warfare*, Center for Strategic and International Studies (Washington, DC, 2 February 2018), accessed at <https://www.csis.org/analysis/return-political-warfare> on 9 October 2018.

Kaldor, M., *New and Old Wars: Organised Violence in a Global Era* (Cambridge: Polity Press, 2013).

Kennan, G. F., *On Organizing Political Warfare*, US History and Public Policy Program Digital Archive, Redacted Document 269, FRUS, 30 April 1948, accessed at <https://digitalarchive.wilsoncenter.org/document/114320> on 22 March 2019.

Kissinger, H., 'Henry Kissinger on the Assembly of a New World Order', *Wall Street Journal*, 29 August 2014.

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



Klapisis, A., *An Unholy Alliance: The European Far Right and Putin's Russia*, Wilfried Martens Centre for European Studies (Brussels, 2015).

Knoke, D., *Political Networks: The Structural Perspective*, Structural Analysis in the Social Sciences (Cambridge: Cambridge University Press, 1990).

Krekó, P. and Gyóri, L., *Russia and the European Far Left*, Institute of Statecraft (London, 2016).

Krekó, P. et al., *Europe's New Pro-Putin Coalition: The Parties of 'No'*, Institute of Modern Russia and Political Capital Institute (New York, 2015).

Krishnan, A., *Military Neuroscience and the Coming Age of Neurowarfare* (London: Routledge, 2017).

Lanoszka, A., 'Russian Hybrid Warfare and Extended Deterrence in Eastern Europe', *International Affairs* 92/1 (2016), 175–95.

Laruelle, M., *Eurasianism and the European Far Right: Reshaping the Europe–Russia Relationship* (Lanham, MD: Lexington Books, 2015).

Libicki, M. C., *What Is Information Warfare?*, Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University (Washington, DC, 1995).

Lord, C. and Barnett, F. R., (eds.), *Political Warfare and Psychological Operations: Rethinking the US Approach* (Washington, DC: National Defense University Press, 1989).

Manjikian, M. M. E., 'From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik', *International Studies Quarterly* 54/2 (2010), 381–401.

Meister, S., 'The "Lisa Case": Germany as a Target of Russian Disinformation', *NATO Review* (2016), accessed at <https://www.nato.int/DOCU/review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm> on 22 March 2019.

Mudde, C., 'Russia's Trojan Horse', *Open Democracy*, 8 December 2014, accessed at <https://www.opendemocracy.net/od-russia/cas-mudde/russia's-trojan-horse> on 22 March 2019.



Newbury, C., *Patrons, Clients, and Empire: Chieftaincy and Over-Rule in Asia, Africa, and the Pacific* (Oxford: Oxford University Press, 2003).

Nimmo, B., *Identifying Disinformation: An ABC*, Institute for European Studies, Issue 2016/1 (Brussels, 2016).

Nissen, T. E., *The Weaponization of Social Media*, Royal Danish Defence College (Copenhagen, 2015).

Noonan, M., 'Re-Inventing Political Warfare', *US News & World Report*, 16 August 2013, accessed at <https://www.usnews.com/opinion/blogs/world-report/2013/08/16/political-warfare-in-a-time-of-defense-cuts> on 22 March 2019.

Nye, J. S., *Soft Power: The Means to Success in World Politics* (New York: Public Affairs, 2004).

Nye, J. S., *The Paradox of American Power: Why the World's Only Superpower Can't Go It Alone* (Oxford: Oxford University Press, 2003), Kindle e-book.

Polyakova, A. and Boyer, S. P., *The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition*, Brookings (Washington, DC, March 2018), accessed at <https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf> on 22 March 2019.

Price, M. E., *Free Expression, Globalism, and the New Strategic Communication* (New York: Cambridge University Press, 2015).

Rácz, A., *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*, Finnish Institute of International Affairs (Helsinki, 2015).

Riefenstahl, L. (producer and director), *Triumph des Willens* [Triumph of the will], Motion picture (NSDAP Reichspropagandaleitung Hauptabt, 1935).

Robinson, L. et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica: RAND Corporation, 2018).

Roselle, L., Miskimmon, A. and O'Loughlin, B., 'Strategic Narrative: A New Means to Understand Soft Power', *Media, War & Conflict* 7/1 (2014), 71–4.

Ross, S. J., *Hitler in Los Angeles: How Jews Foiled Nazi Plots Against Hollywood and America* (New York: Bloomsbury, 2017).

Shadlow, N., 'Welcome to the Competition', *War on the Rocks*, 26 January 2017, accessed at <https://warontherocks.com/2017/01/welcome-to-the-competition/> on 11 February 2017.



Shaheen, J., *Network of Terror: How DAESH Uses Adaptive Social Networks to Spread Its Message*, NATO Stratcom Center of Excellence (Riga, 2015).

Smith, P. A., *On Political War* (Washington, DC: National Defense University Press, 1989).

Soroka, S., 'Media, Public Opinion, and Foreign Policy', *The Harvard International Journal of Press/Politics* 8/1 (2004), 27–48.

Spechler, D., 'Russian Foreign Policy During the Putin Presidency', *Problems of Post-Communism* 57/5 (2010), 35–50.

Stokes, B., *Euroskepticism Beyond Brexit: Significant Opposition in Key European Countries to an Ever Closer EU*, Pew Research Center (7 June 2016).

Szostek, J., 'Defence and Promotion of Desired State Identity in Russia's Strategic Narrative', *Geopolitics* 22/3 (2016), 1–23.

Taillard, M. and Giscoppa, H., *Psychology and Modern Warfare: Idea Management in Conflict and Competition* (Basingstoke: Palgrave Macmillan, 2013).

Toynbee, A. J., *Survey of International Affairs: 1939–1946: Hitler's Europe* (London: Oxford University Press, 1954).

UK, Political Warfare Executive, *The Meaning, Techniques and Methods of Political Warfare*, British National Archives (1942), FO 898/101.

Winnerstig, M. (ed.), *Tools of Destabilization: Russian Soft Power and Non-Military Influence in the Baltic States*, Swedish Defense Research Agency (FOI) (2014).

Zacher, M. W., 'The Territorial Integrity Norm: International Boundaries and the Use of Force', *International Organization* 55/2 (2001), 215–50.

Zgryziewicz, M. R., *Daesh Information Campaign and Its Influence*, NATO StratCom Centre of Excellence (Riga, 2016).

Zgryziewicz, R., *Daesh Recruitment: How the Group Attracts Supporters*, NATO StratCom Centre of Excellence (Riga, 2018).



# About the author

---

**Antonios Nestoras** is a doctoral researcher at the Institute for European Studies at the Vrije Universiteit Brussel. He has also held positions in the International Relations Service of the European People's Party Group in the European Parliament and at the Wilfried Martens Centre for European Studies.

# Credits

---

The Wilfried Martens Centre for European Studies is the political foundation and think tank of the European People's Party (EPP), dedicated to the promotion of Christian Democrat, conservative and like-minded political values.

Wilfried Martens Centre for European Studies  
Rue du Commerce 20  
Brussels, BE - 1000

For more information please visit: [www.martenscentre.eu](http://www.martenscentre.eu)

External editing: Communicative English bvba

Typesetting: Victoria Agency  
Printed in Belgium by Drukkerij Jo Vandenbulcke

This publication receives funding from the European Parliament.

© 2019 Wilfried Martens Centre for European Studies

The European Parliament and the Wilfried Martens Centre for European Studies assume no responsibility for facts or opinions expressed in this publication or their subsequent use.

Sole responsibility lies with the author of this publication.