MCDC Countering Hybrid Warfare Project

The state of current counter-hybrid warfare policy

Information note, March 2019

Introduction

If war is a clash of wills, and humans continue to innovate to gain influence, hybrid warfare (HW) can be regarded as the latest development in the struggle between competitive actors with different interests in the international system.[1] Naturally, as the history of strategy suggests, the success of HW has provoked a counter-reaction among targeted actors, and as strategy is an interactive process, the responses to HW will go through several maturity stages.[2] However, despite considerable interest in HW (and related concepts such as 'grey zone' and 'modern political warfare') there is an absence of efforts to bring together and analyse policies to counter HW.

This paper aims to provide an assessment of the state of current counter HW policy by analysing existing and recommended policies for countering HW. In doing so it seeks to answer five questions.

- What is the balance between offensive and defensive policy measures?

- What instruments of national power are used to implement these policies?

- Are any themes discernible or policies particularly noteworthy among the defensive measures?

- Are any themes discernible or policies particularly noteworthy among the offensive measures?

- What are the casual factors that might explain any observations made from answering the previous questions?

In answering these questions, this paper makes some key observations. First, there is an existing proclivity towards defensive measures, in particular through building resilience in the political and informational spheres of society, supported by increased intelligence-gathering measures. Second, in the implementation of defensive and offensive measures, the informational, diplomatic and military instruments were most used. Of the offensive measures, two key themes were identified: linking the use of different national power instruments and the potential for more assertive use of media and informational capabilities to counter hybrid warfare. Overall, the analysis demonstrates the breadth of options available to policymakers in countering HW. This paper and methodology may serve as a placeholder on the state of counter-HW policy, while inspiring efforts to expand the 'playbook' for countering hybrid warfare.

To provide more detail on these observations this paper proceeds in five steps. First, to understand how the observations were derived,

the methodology is explained. Second, the offence-defence balance is presented and analysed. Next, the instruments of national power used are discussed. The fourth section then focuses specifically on defensive measures and the fifth section on offensive policies. The paper concludes by reiterating the main findings of the analysis.

Methodology

As international security has entered a more competitive era, it seems that revisionist actors are increasingly resorting to ambiguous or 'hybrid' approaches to achieve their objectives without reprisal.[3] To improve existing and future efforts to counter HW, there is a need to bring together lessons from existing research and practice on policy measures, in support of the MCDC Countering Hybrid Warfare (CHW) project.[4] Following MCDC, HW is defined in this paper as 'the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects'.[5] It is centred on the cognitive realm of warfare, and exploits creativity and ambiguity.

To analyse existing and proposed policy measures for countering HW, a framework was established to analyse and compare policies from a range of sources.[6] While not intended to be exhaustive or widely representative, this analysis aims to provide 'food for thought' within the scope of the MCDC CHW project. The framework used for analysis examined three main components. These were:

- whether the policy in question was 'defensive' or 'offensive' in nature;

- the instrument of power used (DIMEFIL)[7]; and

- the type of vulnerability targeted (PMESII)[8].

The basic methodology was to identify and analyse significant recent think-tank and policy publications focussing on HW,[9] extracting suggested policy measures to counter HW and then classifying them

1

---

1 Clausewitz (1989)
2 Luttwak (2001)
3 For an overview of the rise of 'hybrid warfare' and considerations for countering it, see: MCDC (2019).
4 An overview of the CHW project is available at: https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare. The key findings from this research feature in Annex C (p 79-82) of MCDC (2019).
5 MCDC (2017), p 8.
6 The policy analysis framework was devised by Pasi Eronen, Iiris Saarelainen and Simon Källman. Most of the data entry and analysis was performed by Albin Aronsson.
7 DIMEFIL: defence, information, military, economic, finance, intelligence and legal. In the MCDC CHW handbook (MCDC, 2019) the results are presented using MPECI (military, political, economic, civil, information) by equating diplomacy to political, finance to economic, and intelligence/legal to civil.
8 PMESII: political, military, economic, social, infrastructure, information.
9 And related concepts such as 'grey zone', 'modern political warfare', 'sub-threshold', etc. Also see Fridman (2018), p. xi.

according to the main components of the framework above. Table 1 below gives an overview of the range of sources and number of policies analysed. The specific documents analysed can be found at the end of this paper following the bibliography.

Type of publication	Number of publications	Total number of policies
Think tank papers	8	68
European Union and NATO official texts	4	21
MCDC CHW case studies	6	21
Total	18	110

Table 1 – Summary of publication type and number of policy measures

The offence-defence balance

Offence-defence theory is a central element in the study of international politics. In short, the prevalence of instruments of national power which are more conducive to being used offensively can have destabilising effects within the international system.[10] Applied to the contemporary international security environment, it appears that HW may present such a case, where seemingly low cost, low level and (sometimes) unattributable actions are used to achieve effects while avoiding reprisal.

This distinction – between 'offensive' and defensive' actions – is therefore applied to the counter-HW measures proposed in the policy literature as a lens through which to analyse them. The nature of each proposed policy was judged from the perspective of the aggressor in each case. When related to the MCDC CHW framework,[11] defensive options generally relate to deterring hybrid aggressors (mainly through deterrence by denial, for example, through resilience measures) while offensive options generally relate to responding to hybrid attacks (but also cover deterrence by punishment, where the offensive measure can be threatened as punishment). Figure 1 shows the result of this analysis, with the majority (around three-quarters) of proposed policies focussed on defensive measures.
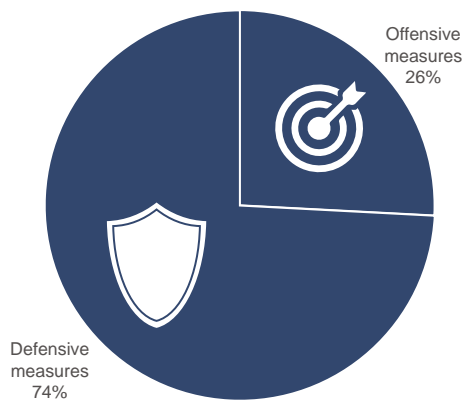
Several factors might explain this preference for defensive measures. First, policy in this area is still at an early stage – so this trend may change over time - but if HW is offensive in nature, it is natural that the countering policies might be focussed on defending against and building resilience towards the threat.

Secondly, the literature views differently the threat stemming from actors that conduct HW, or 'hybrid-aggressors'. Some see HW as a significant threat that is effective at undermining governance and cohesion within and between targeted nations (predominantly in 'the West'). The literature taking this view tends to suggest more offensive options in response to an invidious threat, with the intention to actively target HW actors' own vulnerabilities and raise the costs of engaging in HW.[12] Others see HW merely as a response by the revisionists to the conventional military and normative superiority of the status quo powers, instead suggesting that hybrid aggressors are more opportunistic and experimental in their approach, posing less of a systemic threat. Those in the latter category tend to prefer defensive measures to avoid inflating the threat and exacerbating the problem.[13] This shows that the proportion between offensive and defensive measures often depends on the specific publication, and how each author views the threat posed by HW.

Furthermore, the concept and practise of defensive concepts such as resilience and deterrence are also widely theorised – stemming from Cold War deterrence concepts – and therefore relatively well-understood. While the deterrence of hybrid aggression is not so well conceptualised (e.g. compared to nuclear deterrence), the perception of deterrence as a broader concept, with good prospects for success, appears to influence countries to instinctively prefer defensive to offensive measures. Moreover, many defensive measures are low cost and more predictable than implementing assertive countermeasures.

Finally, current Western strategic culture often tends towards dealing with challenges through a paradigm of risk management, rather than from a perspective of 'strategy', or long-term planning. The latter may be the result of being democracies, where the elaboration and application of strategies are difficult, as the state of domestic politics often changes quickly and occasionally unexpectedly. Related to this, the preponderance of defensive measures might also be explained by a general preference in the international community to avoid being seen as aggressive, either by other nations or their own population.

Figure 1 – Offence-defence balance of hybrid warfare countermeasures
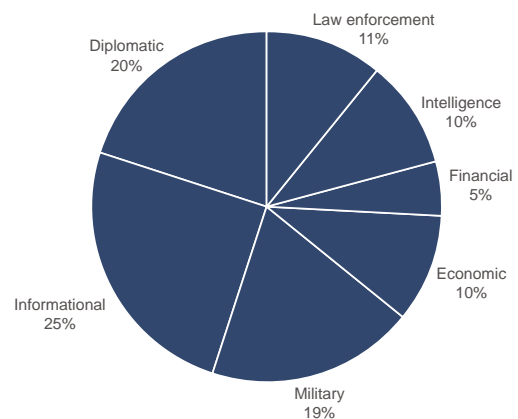

Figure 2 – Instruments of power used (DIMEFIL)

10   See for example: Jervis (1978), Van Evera (1998).
11   See MCDC (2019), p 5.

12   For example in: CSBA (2018)
13   For example in: RAND (2018)

Offensive and defensive measures – instruments of power used

As Figure 2 shows, when executing both offensive and defensive policy measures the most used instruments of national power were the informational, diplomatic and military instruments. If state competition takes place increasingly in the cognitive realm, it follows logically that instruments that can be used to gain an influencing advantage would be used more than others. This helps explain the reliance on the information measures, to counter HW actors who have become more adept at using modern media channels to achieve targeted influence. However, the information instrument does not produce 'news' by itself, but is dependent on the diplomatic, military and other instruments of power to provide the 'raw material' for the information instrument.

Following information, extensive use of the diplomatic instrument is consistent with the common suggestion in the literature that the diplomatic arm of government should lead on responding to and countering HW. This suggestion aligns somewhat with George Kennan's original ideas of conducting 'political warfare'.[14] Following from this, it is unsurprising that the diplomatic instrument, which is fundamentally about influence and persuasion, appears as the main government body that should lead efforts on countering HW. The problem today, however, is that funding and resources for diplomatic capacity is often not aligned with the increasingly important role it must play. For example, this theme is prevalent in relation to what some call the 'militarisation' of U.S. foreign policy.[15] The U.S. case may be an extreme one, but merits consideration by others in their own context.

The military instrument is also suggested across the literature as having the potential to play an important role in countering HW. In most cases, the use of military power in countering HW is connected to signalling, something that, in describing Russia's use of its' military, Mark Galleotti has called 'Heavy-Metal Diplomacy'.[16] Russia, for example, often uses military manoeuvres to disrupt and intimidate (e.g. flying close to other nations' airspace or sailing close to territorial waters). In terms of countering HW, the literature suggests well-communicated military posturing can signal resolve and demonstrate capability and credibility. It also suggests doing so with allies where possible, to maximise the impact and show solidarity.

Also noteworthy in Figure 2 is the low weight given to economic and financial instruments. Financial crime and illicit money flows have become common instruments of hybrid aggression,[17] if only as crucial enablers of other activities. In response the West seemingly often resorts to imposing economic sanctions in response to HW as punishment. There may be two explanations to the relative absence of these measures in the literature. The first is the growing realization that Russia and others have made themselves less vulnerable to this type of sanctions – including sanctions directed at individuals rather than the state per se – and as a result seem to have failed to changed the targeted actor's overall trajectory of behaviour. For example, part of the reason for why sanctions have not worked against Russia is the size of

the country, and its inescapably important role in geopolitics, hydrocarbons and arms sales for countries like China, India and Turkey.[18] Another part is that in the interconnected world isolation may not be possible to the same degree that it was during, for example, the Cold War. Another reason may also be a 'data supply problem'. The HW literature is dominated by people trained in political science, history and strategic studies. Mostly lacking training in more technical fields such as law, finance or economics, there may also exist a relative ignorance about the options available in those areas that could help to counter HW.

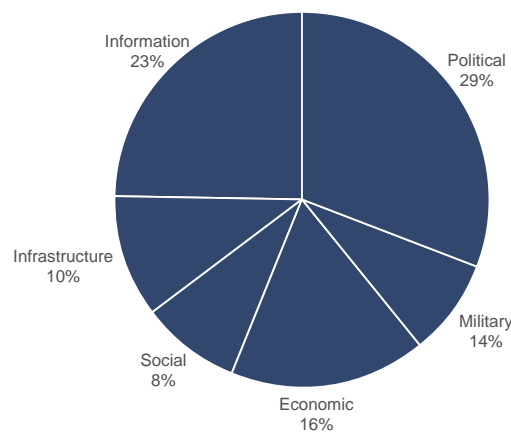## Defensive measures: hardening the target

Figure 3 – Defensive measures – targeted vulnerability

Defensive measures address PMESII vulnerabilities through actions designed to absorb damage and recover from attacks. As Figure 3 shows, the majority of defensive measures proposed were targeted at building resilience in the political and informational spheres of government and society, supported by increased intelligence-gathering measures. One explanation for this is that these are the most vulnerable to attack, by virtue of their openness and the extent to which democratic societies rely on open access to information and transparent political process. These areas may also be the most difficult to protect without compromising the essential nature of open democratic societies. This trend may also reflect the extent to which HW focuses on the cognitive domain of public opinion and political decision making – and the interdependence between these two crucial functions.[19] In this regard, the prominence of the political and informational aspects of countering HW reinforces what is often thought goals of HW – to distract and divide functioning societies.

Two common themes in particular emerged among the defensive policy measures: increasing intelligence gathering and building resilience. The intelligence gathering policies suggested increasing investment to detect and track HW activities by, for example, increasing coordination among countries' intelligence services. More specific examples included the creation of 'counter hybrid support teams' in NATO, and the establishment of a 'Euro-Atlantic Coordinating Council'. Additionally, the setting up of an 'Eastern Hub' for intelligence was also suggested, which would gather, fuse and disseminate information regarding (in this case) Russian activity in the DIMEFIL domains. Increasing intelligence assets would further assist understanding of hybrid aggressor's

---

14   Kennan (1946)
15   For example see: Farrow (2018), RAND (2018).
16   Galleotti (2016)
17   Galleotti (2018)

---

18   Foy (2018)
19   For example: Chivvis (2017), p. 2

decision-making, particularly regarding their intentions around specific attacks. It is worth noting NATO and the EU have already increased investments in intelligence gathering and sharing specifically to deal with HW.[20] No public assessment of the effectiveness of these institutional innovations has yet been made, so it is difficult at this stage to say whether even more investment in this area might be necessary.

The other major theme was resilience. In this analysis, the concept of resilience has been interpreted broadly, related to both materiality such as critical infrastructure, but also government organisational capacity and media resilience. One suggestion was for a common manual or set of guidelines to be developed regarding identifying and protecting critical infrastructure. Another suggestion to increase organisational resilience was for increased training for policy-makers and politicians to improve crisis decision making at national levels in response to HW. However in taking these measures, there is a risk of becoming over-focussed on hybrid threats – either to the detriment of other issues, or seeing everything through the lens of HW and risking 'hybrid paranoia'. This kind of overreaction may play into the hands of hybrid aggressors, infecting and degrading national decision-making more than any attacks could reasonably expect to achieve on their own.

Another resilience trend identified in the analysis was the increased efforts to create societal structures akin to the Cold War concept of 'total defence'. The primary examples are Sweden and Finland, which have increased investment in preparing their societies for crisis or war. Worth mentioning are also Ukraine's efforts in substantially increasing the size of home guard style units with the intention to signal deterrence to any actor contemplating an attack, whether conventional or HW. Creating more paramilitary style units and equipping and training them is something that the Baltic countries have also increasingly done. Although these efforts are localised and context-dependent, it might be worth exploring more widely to understand better if these efforts may constitute more effective deterrence against HW.

It is important to note the limits of resilience as a strategy to counter HW, particularly regarding 'total defence'. In the 1950s, the U.S. contemplated the prospect of potential 'total' war with the Soviet Union, and looked at how policies could be implemented to limit the damage and injury to the U.S. population in case of such conflict. Harold D. Lasswell had earlier written about the idea of the 'Garrison state' in 1941, which can be taken as a warning of going too far in this regard.[21] There is a fine balance between security and freedom. An over-emphasis on the resilience risks altering the character of contemporary societies beyond recognition - politically, societally and even economically. Thus, the idea of building resilience through total defence concepts may only be advisable for the countries most susceptible to hybrid aggression, mostly in terms of geographical proximity to a potential aggressor. In short, despite the threat from HW, trying to protect everything is not a viable way forward – both because there are limited resources to do so, and the consequences may prove counter-productive in undermining

what is valuable and attractive about free and open democratic societies.
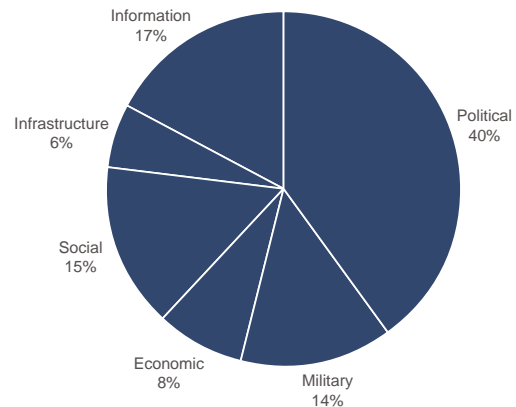
Offensive measures – targeted vulnerability

Figure 4 – Offensive measures – targeted vulnerability

The offensive measures are targeted towards the aggressors' own vulnerabilities, and as conflict and competition remain fundamentally political, it is unsurprising that the political domain is targeted most often – by a significant margin. Measures targeted at political vulnerabilities to counter hybrid warfare are the 'foundation' of any offensive response to hybrid attack. The political nature of states who exploit hybrid warfare often contain elements antithetical to the liberal-democratic model such as centralized power, corrupt elites, control of information flows or lack of transparency, making obvious targets for measures such as anti-corruption and political support to third-party states. However, the very nature of such regimes makes them pre-hardened to such measures. The suggestion to increase political and diplomatic support to third countries (for example those external to EU or NATO in those publications) was relatively common. However, there appears to be a deficit in understanding how these measures will be interpreted by aggressor, including potential for exacerbating existing grievances. Nonetheless, two themes stood out in the proposed policies: 'issue linkage' and going on the media offensive.

First, the notion of creating 'linkages' between specific HW attacks to other domains was suggested, with the aim of competing or responding in a different domain than the original attack was carried out in. For example, a cyber attack on a Western government could be responded to by a surprising conventional military exercise to signal resolve. By being unpredictable, such linkages may encourage caution as the aggressor will be uncertain as to the nature of any response to their aggression. This uncertainty is useful for the purposes of deterrence. Moreover, the idea of linkage is interesting due to that Western countries are seemingly often unable, or at least unwilling, to respond in kind using the same means as the adversary. Linkage might unlock responses that play more to the strengths of the defender.[22] This unpredictability has to be weighed against the risk of unintended escalation, and a risk of miscalculation on behalf of the HW actor. Yet there should also be a realization that timid responses will not lead to any change in behaviour, as recent years appear to have demonstrated. Some degree of 'horizontal' escalation

20   For example, each has now established an intelligence fusion cell focussed specifically on understanding HW.
21   Lasswell (1941)

22   CSBA (2018)

might therefore be worth pursuing to encourage changes in the behaviour of hybrid aggressors.[23]

Second, the idea of going on the 'media offensive' was identified. This included more active steps to introduce new information into 'closed' societies, by more vigorously supporting media that provides counter-information and narratives to the opposing actor's population.[24] Although a revival of structures like the Cold War U.S. Information Agency (USIA) may not be feasible or appropriate, a closer integration of departments and government efforts in the information space, combined with a clearer mission and purpose might bear fruit.[25]

Conclusion

This paper aimed to assess the current state of policy to counter HW by using a simple framework to analyse proposed counter-HW measures in the policy literature. The central finding was the proclivity towards defensive measures. In implementing counter-HW measures the informational, political and military instruments of national power were relied on most heavily. The proportion in the use of these instruments varied between the defensive and offensive measures but there were also significant similarities between them. The majority of defensive measures proposed used these instruments of power to build resilience in the political and informational spheres of government and society, supported by increased intelligence-gathering measures. Proposed offensive measures used these instruments of power to primarily target the political vulnerabilities of hybrid aggressors.

These findings were complemented by analysis of these observations. First, widespread risk-aversion among victims of HW often precludes pursuing more assertive policies in response. Second, familiarity with deterrence as a strategy since the Cold War may contribute to a preference for defensive measures in countering hybrid aggression. Third, while a focus on increasing societal resilience makes sense from a cost-benefit perspective, becoming 'hooked on resilience' risks being counter-productive in the longer term. Finally, the nature of HW – taking place more in the cognitive domain than in the kinetic domain, and exploiting creativity and ambiguity, helps explain the prominence of informational, political and military instruments in countering HW.

The majority of defensive measures were targeted at building resilience in the political and informational spheres of society, supported by increased intelligence-gathering measures. This makes sense insofar as hybrid warfare often targets political decision-making, which is often informed and supported – especially in democratic societies – by freely available public information. Yet these are also the most difficult components of the liberal-democratic societal model to protect. Paradoxically, overdoing resilience and government-led intervention here may undermine the very fabric of society that is trying to be preserved in the first place.

Concerning offensive measures, this analysis perhaps reveals the lack of other options - beyond politics - for horizontal escalation and punitive measures to threaten and cause damage to the

interests of hybrid aggressors. Without these options being developed and deployed, the behaviour of revisionist actors who use HW is unlikely to change. The analysis suggests these options are available – for example, through exploiting horizontal escalation through 'issue linkage' and going on the media offensive.

In the author's view, the most important contribution of the framework assessment and this paper has been to demonstrate the breadth of options available to policymakers in countering HW. This paper and methodology can thus hopefully serve as a placeholder on the state of current counter-HW policy, while inspiring efforts to expand the 'playbook' for countering hybrid warfare.

Bibliography

Armstrong, Matthew (2015), 'No, we do not need to revive the U.S. information agency', War on the Rocks, https://warontherocks.com/2015/11/no-we-do-not-need-to-revive-the-u-s-information-agency/ , Accessed: 2018-11-15

Baudrillard, Jean (1995), The Gulf War Did Not Take Place (Bloomington: Indiana University Press)

Chivvis, Christopher (2017), 'Understanding Russian "Hybrid Warfare" and What Can be Done about it', Testimony presented before the House Armed Services Committee on March 22, 2017.

Clausewitz, Carl von (1989), On War (Princeton: Princeton University Press) Translated by Michael Howard and Peter Paret.

Farrow, Ronan (2018), War on Peace: The End of Diplomacy and the Decline of American Influence (New York: W.W. Norton and Company

Foy, Henry, 'Russian sanctions: why "isolation is impossible', Financial Times, 12 November 2018.

Fridman, Ofer (2018), Russian 'Hybrid Warfare': Resurgence and Politicisation (London: Hurst & Company)

Galleoti, Mark (2016), 'Heavy Metal Diplomacy: Russia's Political Use of its Military in Europe Since 2014 ', European Council of Foreign Relations, https://www.ecfr.eu/publications/summary/heavy_metal_diplomacy_russias_political_use_of_its_military_in_europe_since, Accessed: 2018-10-25

Galleoti, Mark (2018), The Vory: Russia's Super Mafia (London and New York: Yale University Press)

Lasswell, Harold D. (1941), 'The Garrison State', American Journal of Sociology 46, no. 4 (1941), pp 455-68. http://www.jstor.org/stable/2769918. Accessed: 2018-11-16

Luttwak, Edward (2001), Strategy: The Logic of War and Peace (London: Harvard University Press)

Kennan, George (1948), 'Policy Planning Staff Memorandum', http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm, Accessed: 2018-12-05

_____
23   Nyemann and Sorensen (2019)
24   CSBA (2018)
25   Armstrong (2015)

CSBA (2018) Mahnken, Thomas G. & Babbage, Ross & Yoshihara, Countering Comprehensive Coercion: Competitive Strategies Against Authoritarian Political Warfare (Center for Strategic and Budgetary Assessments: Washington D.C.)

MCDC (2017), Understanding Hybrid Warfare. Available at: https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare

MCDC (2019), Countering Hybrid Warfare, 2019. Available at: https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare

Nyemann, Dorthe Bach and Sorensen, Heine (2019), 'Deterrence by Punishment as a way of Countering Hybrid Threats: Why we need to go 'beyond resilience' in the gray zone', MCDC Countering Hybrid Warfare project Information Note. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/783151/20190304-MCDC_CHW_Information_note_-_Deterrence_by_Punishment.pdf

RAND (2018), Robinson, Linda & Helmus, Todd C & Cohen, Raphael S. & Nader, Alireza & Radin, Andrew & Magnuson, Madeline & Migacheva, Katya (2018), Modern Political Warfare: Current Practises and Possible Responses (RAND, Santa Monica, California), Accessible: https://www.rand.org/pubs/research_reports/RR1772.html

Jervis, R. (1978). Cooperation Under the Security Dilemma. World Politics, 30(2), 167-214. Retrieved from http://www.jstor.org/stable/2009958

Van Evera, S. (1998). Offense, Defense, and the Causes of War. International Security, 22(4), 5-43. doi:10.2307/2539239

Publications reviewed for policy framework

Kramer, Franklin, Speranza, Lauren M. (2017), Meeting the Russian Hybrid Challenge: A Comprehensive Strategic Framework (The Atlantic Council of the United States: Washington, D.C.)

Mahnken, Thomas G. & Babbage, Ross & Yoshihara (2018), Countering Comprehensive Coercion: Competitive Strategies Against Authoritarian Political Warfare (Center for Strategic and Budgetary Assessments: Washington D.C.)

Robinson, Linda & Helmus, Todd C & Cohen, Raphael S. & Nader, Alireza & Radin, Andrew & Magnuson, Madeline & Migacheva, Katya (2018), Modern Political Warfare: Current Practises and Possible Responses (RAND, Santa Monica, California), Accessible: https://www.rand.org/pubs/research_reports/RR1772.html

Schaus, John & Matlaga, Michael & Hicks, Kathleen & Conley, Heather & Rathke, Jeff (2018), What Works: Countering Gray Zone Coercion (Center for Strategic and International Studies: Washington, D.C.)

Conley, Heather A. & Stefanov, Ruslan & Mina, James & Vladimirov, Martin (2016), The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe, Center for Strategic and International Studies (CSIS, Washington D.C.) https://www.csis.org/analysis/kremlin-playbook

Gary Schaub Jr, Martin Murphy & Frank G Hoffman (2017), Hybrid Maritime Warfare, The RUSI Journal, 162:1, 32-40, DOI: 10.1080/03071847.2017.1301631

Janda, Jakub (2016), Full-Scale Democratic Response to Hostile Disinformation Operations: 50 Measures to Oust Kremlin Hostile Disinformation Influence out of Europe, European Values think-tank. https://www.kremlinwatch.eu/our-reports/

Treveton, F. Gregory & Thvedt, Andrew & Chen, Alicia R. & McCue, Madeline (2018), Addressing Hybrid Threats, Hybrid CoE, The European Centre of Excellence in Countering Hybrid Threats, Swedish Defense University, Center for Asymmetric Threat Studies, https://www.hybridcoe.fi/publications/addressing-hybrid-threats/

European Commission (2018), Joint Report to the European Parliament, The European Council and the Council on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018

NATO (2018), Brussels Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018

European Commission (2016), Joint Communication to the European parliament and the Council: Joint Framework on countering hybrid threats: a European Union response

European Commission (2018), EU-Western Balkans: Six Flagship Initiatives, Six New Flagship Initiatives to Support the Transformation of the Western Balkans. http://europa.eu/rapid/press-release_IP-18-561_en.htm

MCDC CHW Case Studies – see MCDC (2019), p 73 for a full list.