ENTERING THE GREY-ZONE:
Hybrid Warfare and the Protection of Civilians in Ukraine
June 2013, Spartak, Ukraine: Unexploded ordnances in Eastern Ukraine continue to cause harm to civilians.
ORGANIZATIONAL MISSION AND VISION

**Center for Civilians in Conflict (CIVIC)** is an international organization dedicated to promoting the protection of civilians in conflict. CIVIC envisions a world in which no civilian is harmed in conflict. Our mission is to support communities affected by conflict in their quest for protection and strengthen the resolve and capacity of armed actors to prevent and respond to civilian harm.

CIVIC was established in 2003 by Marla Ruzicka, a young humanitarian who advocated on behalf of civilians affected by the war in Iraq and Afghanistan. Honoring Marla’s legacy, CIVIC has kept an unflinching focus on the protection of civilians in conflict. Today, CIVIC has a presence in conflict zones and key capitals throughout the world where it collaborates with civilians to bring their protection concerns directly to those in power, engages with armed actors to reduce the harm they cause to civilian populations, and advises governments and multinational bodies on how to make life-saving and lasting policy changes.

CIVIC’s strength is its proven approach and record of improving protection outcomes for civilians by working directly with conflict-affected communities and armed actors. At CIVIC, we believe civilians are not “collateral damage” and civilian harm is not an unavoidable consequence of conflict—civilian harm can and must be prevented.

ACKNOWLEDGMENTS

Ewan Lawson, independent researcher on defense and security issues, authored this policy brief. Research for the brief was primarily conducted by Lawson, with support from Beatrice Godefroy (Europe Director), Sergii Doma (Ukraine Senior Military Advisor), and Liza Baran (Ukraine Country Director). The policy brief was reviewed by Marc L inning (Senior Protection Advisor), Lee Sutton (Senior Monitoring and Evaluation Advisor), Shannon Green (Senior Program Director), and Monica Zuraw (Communications Officer).

Elena Abbott copyedited the policy brief, and Jennifer King designed it. CIVIC is deeply grateful to the officials, academics, and civil society leaders who took the time to speak with us and share their perspectives on the influence of hybrid warfare and hybrid threats on the civilian population in Ukraine and, more specifically, in the east of the country. Without their willingness to engage with CIVIC and their commitment to research on various aspects of hybrid warfare, this brief would not have been possible.

We would also like to thank the Foreign Office of the Federal Republic of Germany for supporting CIVIC’s Program in Ukraine and for making this research and report possible.
ACRONYMS:

AFU: Armed Forces of Ukraine
CCTPG: Civilian Casualties Tracking Provisional Group
CHM: Civilian Harm Mitigation
CIMIC: Civil-Military Cooperation
CIVCAS: Civilian Casualty
CIVIC: Center for Civilians in Conflict
EU: European Union
JFO: Joint Forces Operations
IDP: Internally Displaced Person
IHL: International Humanitarian Law
NATO: North Atlantic Treaty Organization
OSCE: Organization for Security and Co-operation in Europe
POC: Protection of Civilians
PTSD: Post-traumatic Stress Disorder
SSM: Special Monitoring Mission
UNICEF: United Nations Children’s Fund
UXO: Unexploded Ordnances
WHO: World Health Organization
## CONTENTS

Organizational Mission and Vision ........................................ iii
Acknowledgments .................................................................. iii
Acronyms ........................................................................... iv
Executive Summary .............................................................. 1
Recommendations ................................................................. 4
Methodology ......................................................................... 6
Understanding Hybrid Warfare: Conceptual Challenges .......... 7
Hybrid Warfare and Hybrid Threats in Practice ..................... 10
Hybrid Activities in Ukraine and Implications for the Protection of Civilians ......................................................... 13
  Military Operations .......................................................... 14
  Information Warfare .......................................................... 15
  Cultural Affairs ................................................................ 17
  Economic Coercion .......................................................... 17
Mitigating and Responding to Civilian Harm in Hybrid Warfare .. 19
  Establishment of the Civil-Military Cooperation Directorate .... 19
  Civilian Harm Tracking ................................................... 19
  Civil-Military Dialogue ..................................................... 21
Conclusion ........................................................................... 22
Endnotes ............................................................................. 23
EXECUTIVE SUMMARY

“Hybrid is the dark reflection of our comprehensive approach. We use a combination of military and non-military means to stabilize countries. Others use it to destabilize them.”

- Jens Stoltenberg, NATO Secretary General

The conflict in Ukraine continues to place a significant burden on civilians, especially with rising tensions and increased ceasefire violations in the beginning of 2021. Over the last seven years, fighting between Ukrainian and Russian-led forces has been responsible for substantial civilian harm in eastern Ukraine. Over 3,300 civilians have been killed, more than 7,000 have been injured, and 3.4 million people in Donbas require humanitarian assistance and protection services. Civilians along the contact line continue to face physical and psychological harm, as well as lasting damage to infrastructure and essential services.

Analyses of civilian harm risks in Ukraine have focused primarily on physical harm—including death and injury—resulting from conventional military activity such as the use of small arms and light weapons, as well as indirect fire from mortars, artillery, and multi-launch rocket systems. As a result of this focus, less attention has been paid to the possible impact of the conflict’s so-called “hybrid nature.” Without careful consideration of hybrid war’s implications on civilians, strategies to protect civilians in eastern Ukraine will continue to be insufficient.

The concept of hybrid war has gained traction in recent years as a way to describe how a number of actors have integrated regular and irregular forces and have taken advantage of the digital revolution to enable the spread of propaganda and disinformation. One of the aims of using a hybrid approach is to stay below the threshold of armed conflict so as to avoid a conventional military response. For example, the Russian occupation of Crimea was conducted with deliberate obfuscation around the identity of the troops involved, causing political leaders in the West to pause just long enough for the occupation to become a fait accompli before an international response could be launched. However, despite emerging as a new trend in warfare, the hybrid concept remains contested and ill-defined among both policymakers and academics, which has hindered efforts to effectively counter hybrid campaigns.

This policy brief seeks to identify the nature of hybrid activity associated with the conflict in Ukraine and to consider its potential impact on Ukraine’s efforts to build and implement a National Strategy on the Protection of Civilians. The focus is primarily on Russian hybrid activities within the conflict, but this is not to suggest that Ukraine is not also using tactics that could be described as hybrid.

Most frameworks assessing the concept of hybrid activities highlight the integration of multiple levels of national power (diplomatic, economic, informational, and military) as a defining component. In the context of Ukraine, two broad forms of hybrid activity can be identified: hybrid warfare and hybrid threats. Hybrid warfare describes activities that are directly linked to the area of military conflict in eastern Ukraine, while hybrid threats are the broader set of coercive activities conducted across Ukraine and against its partners. It is important to recognize that the extent and intensity of hybrid activity has varied between locations and across time during the conflict. At the time of writing, research suggests that the impact of hybrid threats on civilians across Ukraine has been at least as great as that of the hybrid warfare contained in the east.
Our research looked specifically at hybrid activities associated with military operations, information warfare, cultural affairs, and economic coercion in Ukraine. We identified psychological harm as a primary form of civilian harm arising from these hybrid activities, as hybrid actors seek to create and maintain the perception of chaos both in the conflict area and more broadly. Their activities include efforts to undermine relationships between the general population and civilian and military authorities. For example, a series of information campaigns has focused on undermining the credibility of the Armed Forces of Ukraine (AFU), with quantifiable results. Five years after shelling in Mariupol, over 50 percent of the local population still believe that the attack was conducted by the AFU despite the Organization for Security and Co-operation in Europe (OSCE) having identified the non-government-controlled area of Donbas as the firing point. Cyberattacks on critical infrastructure, which weaken public confidence around accessing essential services and basic needs, also contribute to the perception of chaos and failure by local authorities. The goal of these activities is to cause a deterioration in the social environment, breed mistrust and instability, and create an atmosphere where violence will persist. While it has not been possible to map the extent of this psychological harm, there is likely a correlation with cases of physical harm such as suicide, substance abuse, and domestic violence.

Since a large portion of hybrid activity is directed against the civilian population, civil-military cooperation is needed in addition to support from civilian authorities in order to effectively enhance
protection of civilians (POC) efforts. Early in the conflict, Ukraine identified the need for strong links between the AFU and local communities with the formation of the Civil-Military Cooperation Directorate of the Armed Forces of Ukraine (CIMIC). Regular interaction between civilians and members of the military allows the military to better understand protection needs and proactively undertake measures to prevent harm to local populations. Interaction is even more important in a context where a certain level of mistrust exists vis-à-vis the military, as negative perceptions can hamper effective communication channels between civilians and the military. Civil-military cooperation units, including the Civilian Casualty Tracking Provisional Group (CCTPG) that tracks data on civilian harm for the Joint Forces Operations (JFO), are also a valuable capability for countering hybrid activities in Ukraine. Still, there is a need for even closer integration of civil defense capabilities within the military.

One approach to strengthening civil-military cooperation is known as Total or Comprehensive Defense. Already adopted by a number of countries, this strategy seeks to engage the whole of society and build societal resilience through the integration of civil and military defense. While primarily designed to counter external threats to a state, this approach can also contribute to POC by developing individual and community capacity for responding to and recovering from hybrid activities. With this goal in mind, Ukraine should take advantage of opportunities to develop its capacities in crisis management and resilience, such as by incorporating the strategies presented at the NATO-Ukraine Platform on Countering Hybrid Warfare.

As Ukraine continues to build its POC framework, it is crucial for the government and the AFU to consider the potential impact of hybrid activities on the civilian population and adopt a people-centric approach that is aligned with humanitarian principles and compliant with international humanitarian law.
II. RECOMMENDATIONS

To the Government of Ukraine

• Urgently approve the National Strategy on the Protection of Civilians and ensure that any implementation plan integrates responses to both hybrid warfare in the conflict-affected areas and hybrid threats across the country more broadly. The implementation plan should include methods to measure the success of civilian protection tasks in the context of hybrid activities.

• Standardize definitions for hybrid warfare and hybrid threats, and consider a broader definition of civilian harm arising from these hybrid activities. Conduct research to develop a better understanding of the psychological harm caused by these activities, and use this research to inform the action plan to support the National Strategy on the Protection of Civilians. These efforts should not preclude the short-term delivery of assistance and other protection services through local government structures to communities most affected by the conflict.

• Develop a strategic communications plan to sensitize the civilian population to hybrid activities and their impact, as well as to ways in which civilians can contribute to mitigate the negative impacts on POC. This effort needs to extend as far as possible, including into the areas not under government control.

• Ensure that the population has access to reliable sources of information, including by supporting the development of an even more vibrant and free media landscape and, given its reach across the country, resourcing the state broadcaster.

• Introduce measures to ensure the public transparency of funding both for political parties and civil society organizations. Support the continued development of an active and free civil society landscape, ensuring that oversight of organizations’ activities protects freedoms of association and expression. These measures contribute to preserving the NGO space (including those working in humanitarian assistance, protection, and peacebuilding) and mitigate the civilian impact of efforts at “malign” influence designed to contribute to political destabilization and the further deterioration of a protective environment.

• Develop a plan to continue the integration of civil and military defense capabilities, including by considering the “Total Defense” approach adopted in the Nordic and Baltic states. This plan should include a focus on infrastructural and societal resilience while ensuring that civilians retain their protected status and that the humanitarian principles of neutrality, independence, impartiality, and humanity are upheld.

To the Military-Civilian Administrations and Local Governments

• Ensure that local planning and support activities for the protection of civilians consider the impact of hybrid warfare and threats. This endeavor includes developing an understanding of hybrid activities and their potential implications for civilian harm. Structures and processes such as working groups involving the military, civilian authorities, and civil society should be created to share experience, understanding, and best practices.
To the Ministry of Defence and General Staff of the Armed Forces of Ukraine

- Work through the NATO-Ukraine Platform on Countering Hybrid Warfare to standardize definitions for hybrid warfare and hybrid threats. Standardized definitions will ensure a common understanding with partners and provide a basis for integration while implementing the National Strategy on the Protection of Civilians.

- Continue to constrain the use of force in the Donbas region, where it risks harming civilians, and communicate to the population (including in areas not under government control) how this is being done.

- Develop capacity within CIMIC to recognize hybrid activities and engage the civilian population in countering them, including through regular civil-military dialogues. This capacity should be developed while applying the “do no harm” principle and without instrumentalizing civilians, thus reducing the risk of civilian harm.

- Ensure fast and accurate data collection, analysis, and reporting by the CCTPG to minimize opportunities for disinformation.

- Include psychological harm in civilian harm tracking, and ensure such data is shared with other Ukrainian government agencies engaged in protecting civilians.

- Develop strategic communications plans to counter information aspects of hybrid warfare (such as disinformation and propaganda campaigns) at both the national and the local level. These plans should be closely linked to the broader tactical communications strategy delivered by the Ukrainian government.

To International and Ukrainian Civil Society

- Research and analyze civilian harm arising from hybrid activities in Ukraine and other conflict contexts, and use this information to inform the development of strategies to enhance POC.

- Research potential linkages between hybrid activities and civilian psychological harm. Use this research to better understand the causal linkages between them, as well as to illuminate effective approaches to mitigating harm.
METHODOLOGY

The research for this policy brief is based on the combination of a literature review and interviews with a range of experts. The literature surveyed includes material seeking to understand the phenomenon of hybrid warfare, with a particular focus on how the concept applies to Ukraine. The research included analysis of literature on the conflict produced by non-governmental and international organizations. While there has been little written specifically about the intersection between hybrid activities, civilian harm, and approaches to protection, it was possible to derive useful insights from this material.

In addition to the literature review, 12 semi-structured interviews were conducted with experts both in Ukraine and abroad, including experts from NATO and the European Union (EU). The interviews were used to identify interviewees’ understanding of hybrid warfare, particularly in the context of Ukraine, along with their assessment of the implications for protecting civilians from harm and the potential ways in which associated policies could be developed. All interviews were conducted on the basis of anonymity. As with the literature review, material was gathered in both Ukrainian and English. The initial list of potential interviewees was generated through discussions among CIVIC’s local experts and our consultant researcher, with further candidates identified through the literature review.

CIVIC’s research was also supported by material gathered as part of ongoing work on POC in Ukraine. A virtual roundtable specifically addressing hybrid threats and POC was conducted in October 2020 as part of the fifth Civil-Military Cooperation Conference held in Kyiv. Participants included experts from the NATO Strategic Communications Centre of Excellence, the Hybrid Warfare Analytical Group of the Ukraine Crisis Media Centre, the Mohyla School of Journalism, the Institute of World Policy, the Institute of Post-Informational Society, the National Defence University of Ukraine, and the Ukrainian government. The methodology of using a literature review, interviews, and this roundtable discussion allowed for the development of initial recommendations. However, the main limitation of this approach is that it does not include voices and perspectives from individuals living in the conflict zone.

Throughout this policy brief, “POC” refers to all efforts taken to protect civilians from conflict-related harm. “Harm” is further defined as conflict-related death, physical and psychological injury, loss of property and livelihood, and interruption of access to essential services. “Civilian harm mitigation” (CHM) is defined as all measures taken by armed actors to prevent, minimize, and address civilian harm resulting from their own presence, activities, and operations. The intent in this research is not to identify ways to assist states in countering hybrid threats, but to develop and understand ways in which civilians might be protected from such activities.

As will be further discussed in this brief, our research shows that defining hybrid activity remains contentious, although a set of basic elements can be outlined. In summary, hybrid activities use a range of tools, including military activity, economic coercion, and information warfare, to achieve political outcomes, while also limiting the extent of any military response, often through obfuscation and deniability.
IV. UNDERSTANDING HYBRID WARFARE: CONCEPTUAL CHALLENGES

Although it was not the first time the label was used, the first attempt to define the phenomenon of “hybrid war” was arguably Frank Hoffman’s 2007 article, “Conflict in the 21st Century: The Rise of Hybrid Wars.” Based on the experience of the United States and its partners in Iraq and Afghanistan and focusing on the case study of the 2006 conflict between Israel and Hezbollah in Lebanon, Hoffman built on previous debates among academics and practitioners about the definition of “asymmetric” and “fourth-generation” warfare. He defined hybrid conflicts as including “a range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder.” This understanding of hybrid warfare focuses on the blurring of regular and irregular approaches to conflict—an emphasis on its dual nature that is also reflected in other efforts to understand contemporary conflict. In her 2012 book New and Old Wars: Organised Violence in a Global Era, for example, academic Mary Kaldor similarly reflected on these blurred modes of warfare. However, she also emphasized the significance of the globalized economy and the instrumentalization of identity politics.

While Kaldor is not frequently referenced when seeking to understand what hybrid warfare means in the context of a return to state-on-state competition, much of her analysis (perhaps most notably the deliberate targeting of civilian populations) is reflected in how western states and international organizations have defined hybrid warfare.

The concept of hybrid warfare was emphasized within public policy discourse in the aftermath of Russia’s occupation of Crimea in 2014. In part, this emphasis reflected a need to understand how Moscow so effectively managed to surprise the West and cause a degree of cognitive dissonance through obfuscation and attempts at (im)plausible deniability. As the international community sought to explain the occupation through the lens of this new form of warfare, the concept attracted a range of labels, including hybrid, ambiguous, grey-zone, tolerance, threshold, and, most recently, liminal warfare.

Some observers suggest that the phenomenon described by the term “hybrid warfare” is not new—that conflicts have always involved the combination of both regular and irregular forces, as well as the use of other instruments of state power. Based on an analysis of historical case studies from the Roman Empire to the Vietnam War, for example, historian Peter Mansoor argues that, “although there is little new in hybrid war as a concept, it is a useful way of thinking about wars past, present and future.” Other critiques have focused on how the lack of a clear and consistent definition for hybrid warfare gives the impression that it includes all activities by a state and means that the label is sometimes used arbitrarily. As academic Colin Gray has argued, “Hybridity is not hard to find; in fact, it is too easy...hybridity is a conceptual vessel that holds too much water to be analytically useful...”

As Gray suggests, one problem with approaching state activities through this lens is that it risks everything being classified as a hybrid threat. Activities previously considered to be a part of statecraft might now be perceived as bellicose acts, which in turn can trigger escalation. While the purpose of these activities may be aggressive and coercive, labeling all of them as “war” or “warfare” risks focusing solely on military solutions when they might not be the most appropriate.

There are a variety of definitions currently in use to describe both hybrid warfare and hybrid threats, and it is important to note that there continue to be challenges in identifying where hybrid aggression...
fits on the spectrum between normal statecraft and war. NATO, in an article dated August 2019, stated:

“Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations.”

NATO is also working closely with the EU on efforts to counter hybrid threats in the Euro-Atlantic area. The EU External Action Service describes hybrid threats as follows:

“Hybrid threats combine conventional and unconventional, military and non-military activities that can be used in a coordinated manner by state or non-state actors to achieve specific political objectives. Hybrid campaigns are multidimensional, combining coercive and subversive measures, using both conventional and unconventional tools and tactics. They are designed to be difficult to detect or attribute. These threats target critical vulnerabilities and seek to create confusion to hinder swift and effective decision-making.”

The “Concept for the Development of the Defense and Security Sector,” adopted in Ukraine on March 14, 2016, identifies the following characteristics:

“The core format of hybrid warfare against Ukraine is a combination of varied and dynamic actions of the regular [armed] forces of the Russian Federation that cooperate with unlawful armed groups and criminal individuals whose activities are coordinated and implemented in accordance with the single intent and plan with active use of propaganda, sabotage, intentional damage, diversions and terror.”

Despite being used regularly by policymakers and practitioners, hybrid warfare and hybrid threats clearly remain difficult concepts to define. However, according to our research, the following are identifiable as key characteristics:

• Actors seek to achieve political objectives while simultaneously minimizing the risk of a response by staying below the target’s threshold for a conventional military response. While there are formal thresholds, such as NATO’s Article 5, the decision to commit armed forces or take another form of response is ultimately political. Thresholds can therefore be manipulated by an adversary in their own interests.

• Multiple tools of state power are used, including diplomatic, informational, military, and economic power. These are synchronized where possible to achieve strategic political effects against identified vulnerabilities in the target state and society. With the digital revolution, the information environment has arguably become the most significant arena for hybrid aggression.

• Both deception and obfuscation are routinely involved in order to manage the threshold of response.

Hybrid activities that are designed to support conventional military activity on the battlefield, such as targeting families of military personnel with digital propaganda, are part of what could be classified as hybrid warfare. By contrast, activities that have a broader political agenda (beyond the battlefield) or that undermine a supporting state are more accurately described as hybrid threats. In the context of Ukraine, both forms of hybrid activity can be seen in activities directly associated with the continued conflict in the east and south, as well as across the country and against partners.
TOP: March 10, 2014, Crimea: The concept of hybrid warfare was emphasized within public policy discourse in the aftermath of Russia’s occupation of Crimea in 2014.

BOTTOM: March 17, 2014, Kherson Oblast, Ukraine: A Ukrainian serviceman digs a trench at a checkpoint near the village of Streikovo in Kherson region adjacent to Crimea.
HYBRID WARFARE AND HYBRID THREATS IN PRACTICE

Russian hybrid activities in Ukraine are grounded in over a decade of experimentation. In 2007, Estonia suffered a series of major cyberattacks on its banking, government, and media sectors after authorities moved a Soviet-era war memorial from the city center of Tallinn to a park in the outskirts. As part of its operations, Russia took control of Russian-speakers’ grassroots organizations (a process known as astroturfing) and incited outbreaks of violent rioting that caused both physical destruction and civilian harm.\(^7\) Russian actors also frequently referred to the Estonian authorities as “Nazis,” a narrative framing that was later repeated in Ukraine and elsewhere.\(^8\)

A year later, in 2008, Russia first demonstrated the synchronization of hybrid activities with conventional military operations in Georgia. Preparations for the conflict began some weeks earlier with cyberattacks on Georgian hacker groups, with the aim of preventing them from assisting authorities in a potential response. When violent conflict broke out, Russia was able to achieve conventional military victories at the tactical and operational levels, supported by a hybrid campaign that limited the ability of Georgian authorities to communicate with their own people or with the outside world. This hybrid campaign allowed Moscow to dominate the narrative.\(^9\) Over 50 finance, government, and communications websites were targeted and defaced or hit with denial of service attacks. Defacement activities included portraying the Georgian president as Hitler, reiterating the narrative that anyone challenging Moscow is a Nazi. Russian authorities denied responsibility for these cyber-activities, instead attributing them to “patriotic hackers.”\(^10\) However, software to enable both denial of service attacks and website defacement was made available to those “patriotic hackers” by an organized crime group based out of St. Petersburg.\(^11\)

What both of these examples highlight is how the digital revolution—and the increasing dependence of governments, militaries, and broader society on cyberspace—has created an environment conducive to hybrid activities. The nature of cyberspace is such that, whether used as a venue for information operations or to cause physical results, it is difficult for even the most sophisticated actors to ensure that there will not be impacts on civilian networks and, therefore, the potential for civilian harm.

In 2014, Russia’s occupation of Crimea and the support it provided to separatist movements in eastern Ukraine were marked by the combination of regular and irregular combat operations, with Russian forces operating alongside local militias. These activities were directly supported by a campaign of disinformation that sought to cast doubt on the identity of Russian forces—the so-called “little green men”—including formal denials from the Kremlin regarding Russia’s involvement.\(^12\) In addition, the Russian Federation provided support and sponsorship to political protests and conducted cyber-operations that effectively isolated Crimea from the rest of Ukraine. As the conflict wore on and fighting in eastern Ukraine ebbed and flowed, Russia continued to conduct cyberattacks, including attacks targeted at gas supplies and the power grid as part of its economic coercion tactics.\(^13\)
A similar pattern unfolded in subsequent Russian operations in eastern Ukraine. The disinformation campaign spread the narrative that the conflict arose in response to a coup in Kyiv that was supported by the West and enabled the return of fascists to power. The emphasis on fascists returning to power is a recurring theme in Russian information operations, and emphasizes the complicated history of Ukraine’s role in World War II. A French academic and think tank expert has described the use of this narrative as a form of “propaganda intoxication.” Russian campaigns also capitalized on a proposal by the new Ukrainian government to change the country’s language laws, suggesting that the intention was to isolate or eliminate the Russian-speaking population. In response, there were public demonstrations that grew into violence and the occupation of government facilities, most notably in Donetsk and Luhansk oblasts. Moscow provided direct military support to the separatists in the form of training, equipment, and leadership, and supported other non-military activities that targeted Donbas as well as the rest of Ukraine and its western partners more broadly.

While analysis has largely focused on Russian hybrid activity in Ukraine, Ukraine has also seemingly employed hybrid approaches in response to Russian actions. Specifically, for example, Johann Schmid has suggested that “political propaganda, embargoes and disrupting the power supply (Crimea, separatist territories), as well as police and intelligence operations, have been some of Ukraine’s chosen tools.”

Given the danger of all state activity being labeled as hybrid warfare, it is important to focus on the specific hybrid activities that might cause civilian harm, as well as consider the impact of hybrid campaigns on protection efforts. The Henry Jackson Society, a British think tank, developed a framework identifying six key elements of Russia’s current approach to conflict and competition:

<table>
<thead>
<tr>
<th>1</th>
<th><strong>Political Conflict</strong> – Compromising and controlling politicians and interference in elections and referenda.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><strong>Cultural Affairs</strong> – The use and misuse of history and religion in the creation of narratives.</td>
</tr>
<tr>
<td>3</td>
<td><strong>Economic Coercion</strong> – Manipulation of economic links such as fuel transit fees.</td>
</tr>
<tr>
<td>4</td>
<td><strong>Military Operations</strong> – Support to irregular actors including the use of private military companies and so-called volunteers.</td>
</tr>
<tr>
<td>5</td>
<td><strong>Diplomacy and Public Outreach</strong> – Creating narratives about the threat to Russian speakers outside the Russian Federation, as well as the use of “lawfare.”</td>
</tr>
<tr>
<td>6</td>
<td><strong>Information Campaigns</strong> – Narratives designed to destabilize target societies, including by creating rifts between government and society.</td>
</tr>
</tbody>
</table>
Within this framework, component elements may be integrated with one another. For example, cyber-enabled information campaigns can be integrated with military activity. These activities can take place both in the context of hybrid warfare in Donbas and the context of hybrid threats more broadly across Ukraine. Most interviewees observed that, in the case of hybrid warfare in Donbas, the current focus is on keeping the population under control through measures designed to paint the Ukrainian authorities and armed forces as both “incompetent” and “malicious.” In the rest of Ukraine, hybrid threats are designed to keep the country divided and weaken the trust that populations put in local and national authorities. While political in nature, these tactics have implications on the protection environment, especially in the context of an active armed conflict in Donbas.
VI. HYBRID ACTIVITIES IN UKRAINE AND IMPLICATIONS FOR THE PROTECTION OF CIVILIANS

Overall, the primary impact of hybrid activities on civilians is likely to come in the form of psychological harm. A strategy designed to generate a sense of chaos and undermine confidence is likely to negatively impact the mental health of the targeted population. At present, there is little data available to demonstrate causality or even correlation between the different elements of hybrid aggression and mental health, but there is evidence of increased mental health challenges arising from the broader conflict. It has been reported that 96 percent of older people (60 years old and over) living in conflict-affected areas of eastern Ukraine are suffering from conflict-related mental health issues. A separate study from 2017 found that 32 percent of internally displaced persons (IDPs) in Ukraine were suffering from post-traumatic stress disorder (PTSD), with many also having symptoms of stress and anxiety. At the time, some 74 percent of IDPs were not receiving the appropriate mental healthcare. It is generally recognized that psychological harm in the conflict also arises from issues that might not be considered part of the hybrid campaign, including challenges such as displacement, loss of livelihood, and the death or injury of family members. However, these challenges are amplified by the chaos and uncertainty arising from hybrid activities.

The absence of accessible mental healthcare in Donbas also impacts physical health, with individuals resorting to negative coping strategies including alcohol abuse, self-medication, and overloading with work. Such coping strategies can contribute to an increased risk of physical harm, whether accidental harm due to intoxication or through domestic violence. Based on a 2017 law that broadened the understanding of domestic violence and who could be a victim, Ukraine has a strong legal framework for addressing domestic violence. However, there is an underlying culture that makes discussing domestic violence taboo and impacts the extent of public visibility. Still, there is general recognition that domestic violence can be exacerbated by conflict-related trauma, including the sort of activities seen in hybrid aggression. Humanitarian agencies are striving to fill the gaps in addressing mental health needs. Yet, while the United Nations Children’s Fund (UNICEF) is creating a mental health hotline, for example, and the World Health Organization (WHO) is supporting a series of mobile mental health centers, many of those suffering still have significant problems with access.

Further research is needed to quantify the exact scale of civilian harm arising from hybrid aggression in Ukraine, as well as to better understand what threats or occurrences of harm (or combination thereof) are deemed responsible. That being said, it is possible to identify some indicative hybrid activities that lead to civilian harm based on key elements of the Henry Jackson Society’s six-element framework—specifically, activities that fall under military operations, information warfare, cultural affairs, and economic coercion.
Military Operations

Civilian casualties (CIVCAS) continue to arise from military operations in Donbas. The risk of CIVCAS is escalating due to the recent uptick in ceasefire violations and the mobilization of troops and equipment along the contact line. Much of this harm arises from conventional kinetic activity and needs to be addressed through good POC practices by the combatants, such as care in targeting, the selection of an appropriate weapon based on an assessment of proportionality and the risk of civilian harm, and, when possible, ensuring that military equipment is not located among the population.

There are, however, some military operation activities that can be classified as hybrid warfare, including the targeting of Ukrainian soldiers and their families through the mobile phone network. These attacks intercept the voice and text communications of soldiers, and, in some cases, deliver malware to soldiers’ phones in the form of pictures of their spouses or families sent via text message. Some families also receive text messages indicating their spouses or children have been killed or imploring them to ask their loved ones to cease fighting and return home. While psychological operations are a part of conventional military operations, these actions specifically target soldiers’ families with the attendant risk of psychological harm to those civilians. These hacks are also used to geolocate military formations so that they can be struck by artillery and rocket fire. To build resilience against these tactics, the AFU needs to engage with the families of service personnel to sensitize them about potential risks of harm and ensure that they are taking appropriate cyber-security measures.

In the early stages of the hybrid warfare campaign in Donbas, separatist military personnel used civilians to disrupt Ukrainian military activity. Roadblocks were established with crowds of local civilians being directed to first block, then surround, Ukrainian military convoys. On one occasion, a mother placed her child in front of an armored vehicle’s tracks, “screaming hysterically” at the AFU commander that the child would be killed if the vehicle tried to move. In response, the Ukrainian military acted with considerable restraint despite the presence of armed separatists among the crowd. One expert argued that the roadblock was not simply about using the civilian population as “human shields,” but was, rather, a deliberate attempt to create a situation that could generate propaganda opportunities and contribute to divisions between the local people and the Ukrainian authorities. It is essential that the AFU and other Ukrainian military continue to maintain the POC standards they demonstrated in this instance, but the international community also needs to engage with the separatists and their sponsors to ensure that this sort of activity is not repeated and that civilians are not used for such purposes—regardless of whether the civilians would do so voluntarily.

Military activity by the AFU has also been subject to disinformation, particularly with regards to civilian casualties. As recently as November 2020, disinformation was circulated suggesting that, with 75 percent of civilian casualties between January 2017 and September 2020 occurring in non-government-controlled areas, the AFU was deliberately targeting the population as punishment for not accepting the results of the 2014 change of government in Kyiv. While an OSCE report did note that just under 70 percent of civilian casualties had taken place in non-government-controlled areas during that time period, at no point did it attribute responsibility to the AFU. The OSCE further noted that around 25 percent of these incidents actually resulted from civilians mishandling unexploded ordnances (UXOs).

A further example of AFU military activity being the subject of disinformation can be seen in the circumstances surrounding the 2015 shelling of Mariupol. Despite the OSCE identifying that the shelling was initiated from an area not under the control of Ukrainian authorities, 57.2 percent of the local population in 2020 still “literally believe that the city was attacked by the armed forces that are
supposed to protect it.” In the article “Descent into the Mariupol Disinformation Maelstrom,” authors Michael Gentile and Yevgeniya Kuznetsova attribute this belief to disinformation in both the local and international media that was designed to “blur the facts rather than creating a false narrative.”

**Information Warfare**

When asked to identify the main form of hybrid activity present in the conflict in Ukraine, all of those interviewed for this research spoke about the significance of information warfare. One expert highlighted that this kind of warfare does not just mean the use of social media; it also includes the use of mainstream media and the way that stories often travel between the two. Another noted that 40 percent of disinformation incidents recorded by the EU since 2015 occurred in Ukraine.

In addition to broad efforts to spread disinformation with the aim of undermining civilian confidence in the AFU and undermining trust between the Ukrainian authorities and the populations of the non-government-controlled areas, there are also efforts by the de-facto authorities in non-government-controlled areas to deliberately misattribute specific incidents. In June 2019, for example, media in non-government-controlled areas published reports of an attack on a mosque in the north of Donetsk city that came under fire while hosting celebrations for a religious festival. The media reports alleged that the AFU was deliberately targeting Muslim civilians. However, an OSCE report found that while there was some evidence of firing in the area, it came from a direction that the AFU could demonstrate was under separatist control. While the AFU circulated this information quickly, it was not possible to access the population in the non-government-controlled areas. Thus, the false
narrative continued to circulate. Incidents such as this contribute to an environment where eventual reconciliation between parties will be difficult and, therefore, not conducive to POC.

Atrocity stories have a long history in conflict—sometimes for the truth they tell, and sometimes for the role they play in provocative campaigns of disinformation. The power of disinformation is that it is not always possible to tell fact from fiction. In July 2014, for example, Russian television reported that Ukrainian forces had crucified a small boy and dragged his mother to her death behind a tank in the central square of Slovyansk in eastern Ukraine. The source of the story was identified as a local woman married to a separatist militiaman. She was discredited even by her own family, who suggested that she probably sold the story for money. While no evidence could be found to support the allegations, the story was never withdrawn and continues to circulate in the occupied areas.46

Hybrid warfare activities such as these exist at the nexus of military operations and information warfare and have a strong influence on civilian perceptions of the armed forces. Research conducted by CIVIC in 12 communities within the 5-km zone from the contact line in government-controlled areas of Donbas revealed that 43 percent of the population does not generally trust the military; 37 percent feels that the military presence puts their communities at risk of shelling; 40 percent feels uncomfortable interacting with the military; and 36 percent does not have a clear idea about effective mechanisms for communicating with the military.47 With such notable levels of misperception and distrust, understanding the impact of information warfare tactics on civil-military relationships is key for effective implementation of POC in military operations and activities. Currently, civilians are either scared or unwilling to voice their protection concerns to the military, and POC-related problems remain unresolved.

Accurate civilian casualty reporting, recording, and analysis can be seen as a means to counter the propaganda narratives causing civilian harm. Protecting against this form of hybrid activity also requires effective interaction between the military and the civilian population, such as by the establishment of CIMIC, which has increased communication in areas under government control. Consideration also needs to be given to ways in which those living in the non-government-controlled areas can access alternate sources of accurate information.

Alongside the hybrid activities focused on Donbas, it is possible to identify some key themes in the broader information campaign conducted by Russia and Russian proxies in the area. Information activities are often designed to create and manage perceptions. In Ukraine, they are focused on exploiting divisions within society and divisions between society and the state. Perhaps the most obvious of these efforts has been the instrumentalization of ethnicity and, in particular, the targeting of the Russian-speaking population. The narrative has been that the Ukrainian authorities are seeking to suppress the Russian-speaking minority—and even to eliminate it—using right-wing groups with reputations linked to World War II.48 There has also been a smaller campaign targeting dissatisfaction against the Hungarian minority in western Ukraine that has been linked to Russian support.49 It is important to recognize that these narratives have also been aided by the early post-Maidan government’s efforts to change and arguably weaken the legal status of minorities. These information campaigns risk both psychological and physical harm to civilians by fostering fear and the risk of violent reprisals, and the impact of focusing on ethnicity is self-evident in the continuing conflict in eastern Ukraine.
Information campaigns that seek to exploit ethnic tensions clearly have the potential to cause physical and psychological harm, but other information operations carry a similar risk. A local expert on strategic communications highlighted attacks on Ukrainians returning from Wuhan at the beginning of the COVID-19 pandemic as an example. The Ukrainians were attacked by locals on their way to a quarantine location, apparently as a result of a widely distributed fake email purporting to be from the Ukrainian Ministry of Health raising concerns about their return.50

Cultural Affairs

In an effort to undermine Ukraine’s links with western Europe, campaigns have been initiated by Russian-backed actors to promote “traditional” Ukrainian family values over the “liberal values” of the West. These campaigns depict western Europe as aggressively championing the freedom of sexual orientation and gender equality, and they argue that these ideals will disrupt Ukraine’s social stability—a narrative that has also been observed in other states bordering Russia.51 As well as being endorsed by elements of the broadcast media, the Orthodox Church has played a significant role in spreading this message.52 These narratives have been linked to increased violence against the LGBTQ+ community in Ukraine.53

As previously mentioned, Ukraine’s role in World War II plays a significant role in narratives proliferated by Moscow. Ukraine’s history is complex, including both a nationalist element recruited by the Nazis, as well as others acting as partisans and fighting with the Red Army. Moscow seeks to emphasize the former, consistently leveraging Nazi imagery to suggest that Ukraine has been taken over by the right wing.54 This narrative contributes to creating a climate of fear in Donbas that, apart from the potentially harmful psychological effects on the population, also contributes to the continuation of the conflict.

Economic Coercion

The economic costs of the conflict in Donbas have been significant for Ukraine, which lost control of one of its major manufacturing hubs.55 Russia also has the ability to apply further economic pressure through its control of Ukraine’s primary source of power—gas. Gas supplies routed from Russia to Europe through Ukraine contribute to roughly 3 percent of Ukraine’s GDP, and while Russia and Ukraine signed an agreement as recently as December 2019 to guarantee supply, it is still a point of influence for Moscow, which can withhold the resource should it decide there is a suitable pretext.56 A form of economic coercion, this power dynamic can be used to undermine the Ukrainian government’s credibility in the public eye by suggesting that it is unable to guarantee essential fuel supplies.

Economic coercion can also take the form of manipulating access to electricity. In addition to impacting the availability of essential services for the population, the risk of both physical and psychological harm is exacerbated when cyberattacks are conducted against the energy system. Such attacks can even be illegal under IHL in the context of an armed conflict if they deliberately or recklessly target the civilian population. While direct attribution continues to be a challenge in many cases, Russia is known to have been behind several instances. On December 23, 2015, the control centers of three Ukrainian electricity distribution companies were remotely accessed. Hackers took control of the systems and opened breakers at some 30 distribution substations in Kyiv and the Ivano-Frankivsk region. The hack caused more than 200,000 consumers to lose...
power at one of the coldest and darkest times of the year, with potential consequences on civilian health due to exposure to cold. Nearly a year later, on December 17, 2016, a single transmission substation in northern Kyiv lost power as the result of malicious cyber activity. These attacks have been attributed to Russian actors, and in October 2020 the United Stated indicted six Russian intelligence officers for these and other cyberattacks. Nevertheless, it has proved difficult to assess the specific impact of these attacks on civilians, and one expert interviewed emphasized the lack of awareness and preparedness by both society and the authorities to combat such threats. Facilities such as hospitals generally have back-up power sources, and candles can provide alternate sources of light, but the Ukrainian authorities need to improve the cyber security of critical infrastructure and prepare society for the risk of cyberattacks.

May 16, 2011, Kyyivs’ka Oblast, Ukraine: Power lines. Economic coercion, a form of hybrid warfare, can take the form of manipulating access to electricity.
As has been noted, civilians are often the deliberate targets of hybrid activities. Because the AFU has a role to play in addressing the risk of civilian harm in Ukraine, including by strengthening communication between civilians and members of security forces, tracking and analyzing civilian harm incidents, and addressing protection concerns, hybrid activities must be accounted for in its efforts.

Establishment of the Civil-Military Cooperation Directorate

In March–April 2014, in the early stages of conflict in eastern Ukraine, the AFU faced numerous cases of the local Donbas population interfering with military operations, in part because of miscommunication between civilians and the military. This situation was the primary reason for the establishment of Civil-Military Cooperation (CIMIC) structures within the AFU in May 2014. CIMIC officers are now present in each brigade, in all of the AFU headquarters, in the Regional Commands, and alongside the contact line.

CIMIC coordinates the efforts of various stakeholders (the military, security agencies, emergency services, international humanitarian organizations, and other civilian structures) to ensure that civilians affected by the war, including hybrid activities, receive the help and services they need. Their intervention was particularly helpful in February 2020, as the road was cut between Staromaryevka village (in the grey zone) and government-controlled areas after an order from an AFU commander imposed movement restrictions due to COVID-19. This decision essentially prevented civilians from accessing basic services only available in government-controlled areas, such as the food market, schools, healthcare facilities, etc. CIMIC officers coordinated the efforts of multiple organizations and agencies to respond to the problem. Within three days of negotiations with the Joint Forces Operations headquarters (JFO HQ) and the Regional Command, a solution was found to reinstate the Staromaryevka civilians’ access to basic needs.

CIMIC’s ability to quickly respond to protection issues also has the potential to positively influence civilians’ trust in the AFU and therefore mitigate future harm from hybrid activities. Disinformation campaigns negatively depicting the AFU, for example, may be less persuasive or believable.

Civilian Harm Tracking

On December 29, 2018, with the support of CIVIC, the AFU established the Civilian Casualty Tracking Provisional Group (CCTPG)—a unit tasked to collect information on harm inflicted on the civilian population as a result of the armed conflict. The CCTPG analyzes data on civilian harm and provides analytical reports to military commanders to better inform their decisions on preventing civilian casualties and mitigating future harm. The head of the CCTPG at the AFU pointed at the preventive function of this mechanism: “I believe that a fully functional CCTPG may contribute to decreasing the number of CIVCAS. But I would stress the prevention factor. If I observe some bad practices, I had better undertake some preventative action and work with the military, trying to prevent any harm to civilians.”

VII. MITIGATING AND RESPONDING TO CIVILIAN HARM IN HYBRID WARFARE
In the context of hybrid activities, the AFU can use the CCTPG and other civilian harm tracking mechanisms to counter the practice of CIVCAS manipulation within information operations. An example of this use comes from an incident that took place in February 2021. Two civilians were injured at the defense position of an AFU formation when they were shot at after their vehicle entered a forbidden area. No rules of engagement were violated by the military, and medical care was immediately provided to the civilians—although one of them died in the military ambulance while in transport to the hospital. The incident was properly documented by the CCTPG, and within 12 hours the JFO HQ published a report that was then corroborated by the OSCE Special Monitoring Mission (OSCE SMM). The prompt response by the AFU, including tracking and analyzing the incident using the CCTPG, reduced the risk of the incident being used for disinformation.

Civilian harm tracking and mitigation by the AFU provides the military with an opportunity to minimize the effect of the enemy’s hybrid warfare tools—especially information warfare—and to reduce both physical and psychological harm to civilians. These civilian harm mitigation (CHM) mechanisms may also contribute to improved trust between civilians, the AFU, and the Government of Ukraine, leading to better prospects for identifying a lasting solution to the conflict.
Civil-Military Dialogue

An effective way to reduce misperceptions and distrust between militaries and civilians—vulnerabilities that can be exploited by hybrid activities—is to encourage regular communication and dialogue between the two groups so that they can directly discuss protection concerns. With support from CIVIC, civil-military dialogues began in 2020 in 11 communities along the contact line. During these dialogues, civilians and members of the military have discussed a wide range of issues, including ways to improve communication between the military and community, joint initiatives to raise mine awareness, actions to take in case of emergency, and concerns about military behaviors such as carrying weapons in public places or violating COVID-19 quarantine norms.

According to feedback received from dialogue participants, both civilians and the military feel more confident afterward, reporting that they now feel comfortable directly engaging in discussions on more sensitive protection issues. Increased communication between civilians and the military also means that civilians can gain access to information firsthand rather than relying solely on external media messages.
CONCLUSION

Conceptually, hybrid activity is fairly broad, involving multiple levers of power and often designed to operate below the threshold of armed conflict. The nature of hybrid activity, including both hybrid warfare and hybrid threats, means that it can be difficult to directly link specific incidents of civilian harm to these activities even though they often target the civilian population. In Ukraine, the primary form of Russian-sponsored hybrid activity is information warfare and, in particular, disinformation campaigns. These campaigns are designed to ensure the continuation of conflict in the east while undermining confidence in the state authorities more broadly—a situation that leads to both psychological and physical civilian harm.

There are actions that the Ukrainian military and government can and should take to mitigate the risks of civilian harm stemming from Russian hybrid activities. The Ukrainian government needs to prioritize the approval of the National Strategy on the Protection of Civilians and develop an implementation plan that includes actions to mitigate the risk of civilian harm from hybrid activities. These efforts should include consideration of the information environment as well as ways to support the population in getting access to credible sources of information, particularly in conflict-affected areas. The importance of building societal resilience to counter hybrid activity also needs to be reflected in measures taken by authorities at the local level, including through regular dialogues between civilians, local authorities, and the military. Additionally, the AFU must ensure that it continues to observe the highest standard of conduct with regards to avoiding civilian casualties in its military operations. Support to the population from CIMIC, as well as fast and accurate civilian casualty reporting, are important measures to mitigate the risk of civilian harm. Still, further research by both Ukrainian authorities and civil society is required to confirm the precise nature of the causality between hybrid activity and civilian harm, particularly in regards to psychological harm.

There are actions that the Ukrainian military and government can and should take to mitigate the risks of civilian harm...
ENDNOTES


4 “Regular forces” refers to the armed forces of a state, whereas “irregular forces” refers to state militias or non-state actors.

5 The threshold at which a state will consider a conventional military response can be formal, as in NATO’s Article 5. There is also a legal threshold in the definition of “armed conflict” within international humanitarian law. However, a state’s response is more generally a reflection of political will.


7 In the context of shocks such as natural disaster, failure of critical infrastructure, or a hybrid or armed attack, NATO states that resilience is “a society’s ability to resist and recover easily and quickly from such shocks and combines both civil preparedness and military capacity.” See NATO, “Resilience and Article 3,” November 16, 2020, https://www.nato.int/cps/en/natohq/topics_132722.html#text=Resilience%20is%20a%20society%20s%20ability%20to%20recover%20easily%20and%20quickly%20from%20shocks%20and%20combines%20both%20civil%20preparedness%20and%20military%20capacity.


11 Colin S. Gray, “Categorical Confusion? The Strategic Implications of Recognizing Challenges Either as Irregular or Traditional,” Strategic Studies Institute, February 2016, 16.


16 CIVIC interview with NATO Senior Researcher on Strategic Communications, #6, conducted online, August 2020.


19 Ibid., 63–64.


21 David Kilcullen, The Dragons and the Snakes: How the Rest Learned to Fight the West (London: Hurst, 2016), 145.

22 Lawrence Freedman, Ukraine and the Art of Strategy (Oxford: Oxford University Press, 2019), 89.


24 Freedman, Ukraine and the Art of Strategy, 78.

25 CIVIC interview with French academic and think tank expert, #1, conducted online, August 2020.


29 CIVIC interview with researcher and policy adviser from Ukraine focused on strategic communication, #5, conducted online, August 2020, CIVIC interview with senior researcher and think tank expert from Estonia focused on hybrid conflict, #7, conducted online, August 2020.

30 A senior researcher and think tank expert from Estonia emphasised this point and the challenge of demonstrating causality without further research. See CIVIC interview with senior researcher and think tank expert from Estonia focused on hybrid conflict, #7, conducted online, August 2020.


CIVIC interview of national security official from eastern European state, #4, conducted online, August 2020.

See the Joint Forces Operation report on the incident at CIVIC survey report, September 2020. The survey was conducted by IFAK Inc. in July–August 2020 via face-to-face interviews.

Censor.net, “April 16, 2014. The 25th airborne brigade occupies Kramatorsk airport. 6 vehicles are taken by militants],”

CIVIC interview with researcher and disinformation fact-checker from Ukrainian civil society, #8, conducted online, August 2020.

Donghui Park and Michael Walstrom, “Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks,” The Henry M. Jackson School of International Studies: University of Washington, October 11, 2017,


Censor.net, “April 16, 2014. The 25th airborne brigade occupies Kramatorsk airport. 6 vehicles are taken by militants],”

CIVIC interview with French academic and think tank expert focused on hybrid conflict, #1, conducted online, August 2020.


Gentile and Kuznetsova, “Descent into the Mariupol Disinformation Maelstrom.”

CIVIC interview with researcher and policy adviser from Ukraine focused on strategic communication, #5, conducted online, August 2020.

CIVIC interview with European Union official focused on strategic communications policy, #9, conducted online, August 2020.

CIVIC interview with researcher and disinformation fact-checker from Ukrainian civil society, #8, conducted online, August 2020.


CIVIC interview of national security official from eastern European state, #4, conducted online, August 2020.


CIVIC interview with senior researcher and think tank expert from Estonia focused on hybrid conflict, #7, conducted online, August 2020.


CIVIC interview with national security official from eastern European state, #4, conducted online, August 2020.


CIVIC interview with senior researcher and think tank expert from Estonia focused on hybrid conflict, #7, conducted online, August 2020.

CIVIC interview with high-level CIMIC officer in the Armed Forces of Ukraine, #12, conducted in person, August 2020.

July 24, 2018, Zolote, Ukraine: Two men walk down a street lined with power lines in Zolote.