## MCDC Countering Hybrid Warfare Project:

# Understanding Hybrid Warfare

MCDC January 2017

MCDC
Multinational Capability Development Campaign

## MCDC Countering Hybrid Warfare Project:

# Understanding Hybrid Warfare

## A Multinational Capability Development Campaign project

## Distribution statement

This document was developed and written by the contributing nations and international organizations of the Multinational Capability Development Campaign (MCDC) 2016-17. It does not necessarily reflect the official views or opinions of any single nation or organization, but is intended as recommendations for multinational partners' consideration. Reproduction of this document is authorized for personal and non-commercial use only, provided that all copies retain the author attribution as specified below. The use of this work for commercial purposes is prohibited; its translation into other languages and adaptation/modification requires prior written permission. Questions or comments can be referred to: mcdc_secretariat@apan.org

## Primary authors

Dr. Patrick J. Cullen
Senior researcher
Norwegian Institute of International Affairs
pc@nupi.no

Erik Reichborn-Kjennerud
Research fellow
Norwegian Institute of International Affairs
er@nupi.no

## Linkages

This document is accompanyed by the Baseline Assessment document and detailed case studies. These are available at: https://wss.apan.org/s/ME/mcdc2015-2016/CHW/SitePages/Home.aspx?RootFolder=%2Fs%2FME%2Fmcdc2015%2D2016%2FCHW%2FShared%20Documents%2F00%5FCHW%5FFinal%5FProducts&FolderCTID=0x0120006A81584276FCD643AA9F46228ED57281&View={142DCC1F-EF3E-4364-B46B-C1AE4230F9DD}

For access, please contact the authors detailed above.

# Executive summary

The international consensus on 'hybrid warfare' is clear: no one understands it, but everyone, including NATO and the European Union, agrees it is a problem. This report takes the view that in order to solve a problem, one must first understand it. It sets out a framework – developed under the Multinational Capability Development Campaign (MCDC) Countering Hybrid Warfare (CHW) project – to help nations understand, detect and respond to hybrid warfare.

The first step was to establish a baseline understanding of hybrid warfare based on the latest literature and empirical evidence. The Baseline Assessment is intended to clear up conceptual confusion regarding hybrid warfare, and establish a common language for describing the concept. It describes hybrid warfare as the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects.

The relative novelty of hybrid warfare lays in the ability of an actor to synchronize multiple instruments of power simultaneously and intentionally exploit creativity, ambiguity, non-linearity and the cognitive elements of warfare. Hybrid warfare – conducted by state or non-state actors – are typically tailored to remain below obvious detection and response thresholds, and often rely on the speed, volume and ubiquity of digital technology that characterizes the present information age. It concludes that hybrid warfare is already prevalent and widespread, is used by state and non-state actors, and is likely to grow as a challenge, justifying new efforts by nations to understand the threat it presents. The Baseline Assessment is included as an accompanying document to this report, but its findings are built on and referred to throughout.

The second part of the MCDC CHW project was to develop a framework to help nations understand and think about how to deter, mitigate and counter this threat. The main body of this report is dedicated to developing and describing this framework – known as the Analytical Framework. The framework is based on three parts: critical functions and vulnerabilities; synchronization of means; and effects and non-linearity. While these three parts are separated for the purpose of analysis, they must be understood as a complete system: hybrid warfare is a textbook case of 'the whole being greater than the sum of its parts'. The framework is then developed into a visual tool to help the reader understand the concept. The framework benefits from a set of detailed reports on the following five case studies: Iran's activity in Syria; Russia's use of gas and lending instruments in the Ukrainian conflict; ISIL's activities in Syria and

Iraq; hybrid warfare in an urban context; and Russia's use of cyber capabilities. These case studies are exploratory in nature, but provide both the evidence to underpin the Analytical Framework, and a means to validate and refine the framework through empirical examples. The visual tool is used to illustrate some of the examples in the case studies. This helps the reader to better understand the character of hybrid warfare by populating the visual tool with real-world examples.

Finally, based on the Analytical Framework and the insights it yields – some basic recommendations are provided to assist national governments to better prepare for hybrid warfare and the threats it poses to their interests. These are reiterated below.

## Policy recommendations

- Hybrid warfare is designed to exploit national vulnerabilities across the political, military, economic, social, informational and infrastructure (PMESII) spectrum. Therefore as a minimum national governments should conduct a self-assessment of critical functions and vulnerabilities across all sectors, and maintain it regularly.

- Hybrid warfare uses coordinated military, political, economic, civilian and informational (MPECI) instruments of power that extend far beyond the military realm. National efforts should enhance traditional threat assessment activity to include non-conventional political, economic, civil, international (PECI) tools and capabilities. Crucially, this analysis must consider how these means of attack may be formed into a synchronized attack package tailored to the specific vulnerabilities of its target.

- Hybrid warfare is synchronized and systematic – the response should be too. National governments should establish and embed a process to lead and coordinate a national approach of self-assessment and threat analysis. This process should direct comprehensive cross-government efforts to understand, detect and respond to hybrid threats.

- Hybrid threats are an international issue – the response should be to. National governments should coordinate a coherent approach amongst themselves to understand, detect and respond to hybrid warfare to their collective interests. Multinational frameworks – preferably using existing institutions and processes – should be developed to facilitate cooperation and collaboration across borders.

# Contents

> “Our common understanding of hybrid warfare is underdeveloped and therefore hampers our ability to deter, mitigate and counter this threat.”

# Introduction

Our common understanding of hybrid warfare is underdeveloped and therefore hampers our ability to deter, mitigate and counter this threat. The Multinational Capability Development Campaign (MCDC) Countering Hybrid Warfare (CHW) project is designed to address this shortcoming by developing an analytical framework for understanding hybrid warfare. Its purpose is to increase national and multinational policymakers' and armed forces' understanding of hybrid warfare in order to develop possible solutions to this threat.

To this end the MCDC CHW project is comprised of two primary interconnected deliverables: the Baseline Assessment[1] and the Analytical Framework. The MCDC CHW project also has a set of secondary outputs – a series of case studies of hybrid warfare – designed to test and enhance the validity of the Analytical Framework model by exposing it to empirical examples. The case studies were designed using a qualitative and comparative methodology to:

- ensure each case study was organized to allow testing of the Analytical Framework model; and

- allow for the development of tabulated comparative matrices of hybrid warfare across the case studies.

## The Baseline Assessment

The Baseline Assessment completes two specific tasks. First, it clears up the conceptual confusion and vocabulary related to the term hybrid warfare and creates a common 'language' while serving as a starting point for understanding and analyzing the problem. The second task of the Baseline Assessment is to identify gaps in our understanding of hybrid warfare and to draw out common characteristics that could then be developed into generic analytical components to serve as the basis for the second deliverable, the Analytical Framework.

## The Analytical Framework

The Analytical Framework has four primary tasks.

- First, it provides a pragmatic and policy-oriented heuristic model for understanding hybrid warfare composed of three interlocking parts.

[1] A link to the Multinational Capability Development Campaign (MCDC) Countering Hybrid Warfare (CHW) Baseline Assessment document can be found in the linkages section on page 2.

These include the:

- defender's critical functions and vulnerabilities;
- attacker's synchronized use of multiple means and exploitation of horizontal escalation; and
- linear and non-linear effects of an hybrid warfare attack.

- Second, it provides graphic examples, and explains how these visualizations aid our understanding of the threat.

- Third, the Analytical Framework provides a demonstration of its application to a specific context.

- Fourth, it provides recommendations for developing future solutions to deter, mitigate and counter hybrid warfare threats.

# Describing hybrid warfare

Although both state and non-state actors engage in hybrid warfare they vary widely in their means and actions. That being said, they all exhibit the capability to synchronize various instruments of power against specific vulnerabilities to create linear and non-linear effects. By focusing on these characteristics of a hybrid warfare actors' capabilities, together with the target's vulnerabilities in these areas and then overlaying these with the means and effects, the Baseline Assessment was able to create a generic description of hybrid warfare. It describes hybrid warfare as: the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects.[2]

The Baseline Assessment concluded that hybrid warfare is asymmetric and uses multiple instruments of power along a horizontal and vertical axis, and to varying degrees shares an increased emphasis on creativity, ambiguity, and the cognitive elements of war. This sets hybrid warfare apart from an attrition-based approach to warfare where one matches the strength of the other, either qualitatively or quantitatively, to degrade the opponent's capabilities.

[2] Because of the difficulties of agreeing a common definition of the term 'hybrid warfare', this project focused on describing, rather than defining, the challenge. For a richer discussion of hybrid warfare see the MCDC CHW Baseline Assessment document accessible via the link on page 2.

Figure 1 shows how a hybrid warfare actor can synchronize its military, political, economic, civilian, informational (MPECI) instruments of power to vertically and horizontally escalate a series of specific activities to create effects. It also shows how a hybrid warfare actor can either vertically escalate by increasing the intensity of one or many of the instruments of power, and/or horizontally 'escalate' through synchronizing multiple instruments of power to create effects greater than through vertical escalation alone.

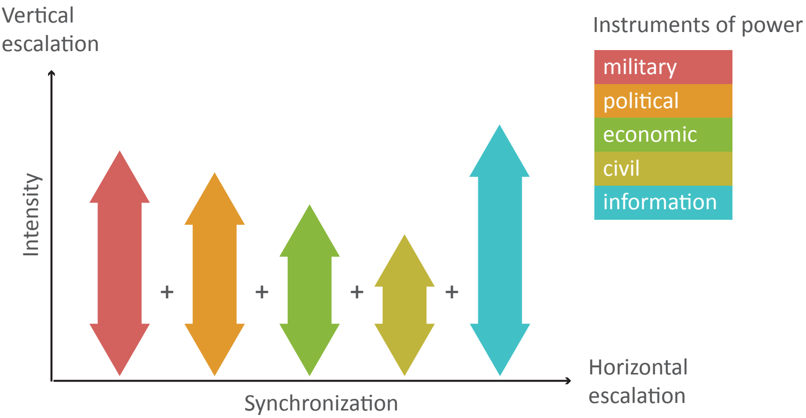


Figure 1 – Hybrid warfare escalation

The key is to understand that the different instruments of power are used in multiple dimensions and on multiple levels simultaneously in a synchronized fashion. This type of thinking allows the hybrid warfare actor to use the different MPECI means at their disposal to create synchronized attack packages (SAPs) that are specifically tailored to the perceived vulnerabilities of the target system. The instruments of power used will depend on the capabilities of the hybrid warfare actor and on the perceived vulnerabilities of its opponent, as well as the political goals of the hybrid warfare actor and its planned ways to achieve those goals. As with all conflicts and wars, the character of hybrid warfare depends on the context.

# Understanding hybrid warfare

Given this view, understanding a hybrid warfare adversary does not lend itself solely to a traditional threat analysis based on its capability and intent for a number of important reasons.

- First, hybrid warfare uses a wider set of MPECI tools and techniques that one usually will not look at in traditional threat assessments.

- Second, it targets vulnerabilities across societies in ways that we do not traditionally think about.

- Third, it synchronizes its means in novel ways. For example, by only looking at the different instruments of power an adversary possesses, one cannot necessarily predict how and to what degree they might be synchronized to create certain effects. Thus, the functional capabilities of a hybrid warfare adversary, although important, will not necessarily provide the right information to understand the problem.

- Fourth, hybrid warfare intentionally exploits ambiguity, creativity, and our understanding of war to make attacks less 'visible'. This is due to the fact that they can be tailored to stay below certain detection and response thresholds, including international legal thresholds, thus hampering the decision process and making it harder to react to a hybrid warfare attack.

- Fifth, relatedly, and arguably more than conventional types of warfare, a hybrid warfare campaign may not be seen until it is already well underway, with damaging effects having already begun manifesting themselves and degrading a target's capability to defend itself.

The issues described above provide the basis for expanding the traditional enemy-centric threat analysis. To this end, the Analytical Framework model focuses on the vulnerabilities of the defender, the ability of the hybrid warfare attacker to synchronize a wide variety of its capabilities during its attack, and the effects created as a result of these actions against specific vulnerabilities of its intended target.

# Building the Analytical Framework: understanding its three key categories

The Analytical Framework is based on three discrete, yet interlocked, categories. While analytically separated here, they need to be understood in concert, because the sum of hybrid warfare is greater than each individual part. They are:

- critical functions and vulnerabilities;
- synchronization of means (horizontal escalation); and
- effects and non-linearity.

## Critical functions and vulnerabilities

Critical functions are activities or operations distributed across the political, military, economic, social, information, infrastructure (PMESII) spectrum which, if discontinued, could lead to a disruption of services that a working system (for example, a state, its society or a subsection thereof) depends on. Critical functions can be broken down into a combination of actors (for example, individuals or organizations), infrastructures (for example, ‘critical’ national power grids) and processes (for example, legal/jurisdictional, technical, political).

**Example: exploiting vulnerabilities**

The deep sectarian, ethnic and economic divisions in Syrian society were exploited by both Iran and ISIL with a view to achieving their strategic objectives.[3]

All critical functions have vulnerabilities that present a hybrid warfare opponent/actor with the possible conditions for exploitation, depending on the means at its disposal. However, it is important to realize that not all vulnerabilities necessarily present themselves as opportunities for an opponent to exploit. Alternatively, an adversary may choose not to exploit a particular vulnerability depending on its intentions. Furthermore, vulnerabilities within critical functions may not be known to a target system (for example, unknown vulnerabilities such as a zero-day cyber attack), and may only present themselves as events unfold.

[3] Annex B and D of the Baseline Assessment document (see page 2 for link).

Countering hybrid warfare demands an assessment of critical functions, the interdependencies of these functions and their vulnerabilities. This 'look at ourselves' requires a risk assessment process that is sensitive to vulnerabilities across civil society and not just within the military or security sector. While such an assessment is valuable on its own regardless of hybrid warfare, understanding hybrid warfare as a type of action that is specifically tailored to vulnerabilities means that hybrid warfare cannot be understood without reference to those vulnerabilities. The results of this hybrid warfare self-assessment will vary considerably from one target system to the next, making each assessment unique and highly contextual.

**Example: exploiting vulnerabilities**

In May 2014 the Russian hacker group CyberBerkut exploited cyber vulnerabilities (routers, software and hard drives) of the Ukranian National Election Commission to undermine the credibility of the elections.[4]

## Synchronization of means and horizontal escalation

Synchronization is the ability of a hybrid warfare actor to effectively coordinate instruments of power (MPECI) in time, space and purpose to create the desired effects. The ability to synchronize both military and non-military means simultaneously within the same battlespace is considered a key characteristic of a hybrid warfare actor.

**Example: synchronization**

In autumn 2013 Iran synchronized terrorist threats, cyber attacks and propaganda to influence the calculation by the US and allies in order to deter external intervention in Syria.[5]

Synchronization allows the hybrid warfare actor to 'escalate' or 'de-escalate' horizontally rather than just vertically, thus providing further options for the attacker. For example, by escalating along the horizontal axis (MPECI spectrum) through synchronization of different means, a hybrid warfare actor can stay below certain detection and response thresholds. By using this method, they can apply as much, or even more, coercion than if they were to escalate one instrument vertically. In other words, through horizontal escalation a hybrid warfare actor can create effects similar, or even greater, than applying overt coercion through, for example, the military or political instrument of power, because of its force multiplying effects.

[4] Annex F of the Baseline Assessment document (see page 2 for link).

[5] Annex B of the Baseline Assessment document (see page 2 for link).

Synchronization also allows for de-escalation of one or more instruments of power and/or switching between means while keeping the overall escalation at a certain level. Also, one instrument can be used for compensatory measures, as a carrot, while others are used as coercive, as a stick.

In essence, synchronization and horizontal escalation provides the attacker with more options than if they were to use unsynchronized vertical escalation alone. Crucially, much of what is done in the horizontal axis can be ambiguous – either hidden from view (for example, cyber operations), conducted with unclear intent (such as investing in foreign critical infrastructure) or not readily definable as a hostile and aggressive act (instigating non-violent protest, for example). Synchronization has several advantages for the attacker:

- the ability to tailor means and vulnerabilities to effects;
- the ability to use coercion while staying below the target's detection thresholds;
- the ability to use coercion while staying below the target's response thresholds; and
- easier to simultaneously escalate and de-escalate.

**Example: synchronization**

In parallel with setting up secret military training camps, ISIL established missionary offices spreading their Salafi message in local communities as well gathering information on all social structures. This information was utilized to target political and military opposition.[6]

## Effects and non-linearity

In hybrid warfare, effects are understood as a change of state of an entity. They are the results of synchronized actions tailored against specific vulnerabilities of a target system. The ability of a hybrid warfare actor to synchronize means against specific vulnerabilities to create effects means that one cannot readily discern a linear causal chain of events. The more elements that are in the mix the more difficult causality becomes.

**Example: non-linear effect**

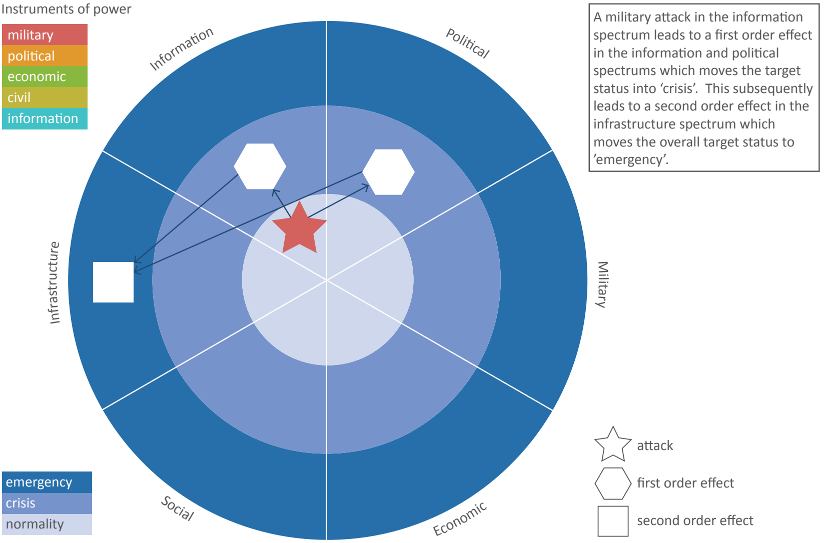
The unforeseen consequence of persuading Ukraine to abandon EU negotiations was the Maidan protest and the ouster of the President, which Russia adapted to and capitalized on.[7]

[6] Annex D of the Baseline Assessment document (see page 2 for link).

[7] Annex C of the Baseline Assessment document (see page 2 for link).

Action A does not necessarily lead to outcome B. Moreover, the same action may cause a different effect in a different context. Although it is possible to analyze effects through consequence/impact analysis of very specific actions taken against specific targets (for example, blowing up a dam will lead to flooding which will result in X amount of damage given the amount of water in the reservoir) this does not provide an indication of how one might be attacked. While some form of causality and second and third order effects might be visible in hindsight, non-linearity makes analysis, and especially prediction based on past empirical examples, extremely difficult. The problem with non-linear effects is that they can only be 'seen' once they have manifested. They are by definition unpredictable. This also means that the adversary cannot plan or control these effects. More importantly, they will need to be highly adaptable if they are to be ready to capitalize on the different effects of their actions as they occur.

## Visualizing hybrid warfare using the Analytical Framework



A military attack in the information spectrum leads to a first order effect in the information and political spectrums which moves the target status into 'crisis'. This subsequently leads to a second order effect in the infrastructure spectrum which moves the overall target status to 'emergency'.

Figure 2 – Visualizing hybrid warfare

For heuristic purposes, Figure 2 demonstrates how each of the three elements of hybrid warfare might be represented within a single graphic.

- **Critical functions and vulnerabilities.** The target of a hybrid warfare attack is represented by the pie chart divided into PMESII sectors (indicated along the outer ring). This shows the potential scope and breadth of operations of a hybrid warfare attacker. It also emphasizes the need of each state to consider mapping out its own critical functions and vulnerabilities across PMESII in terms of its status: normality, crisis and emergency.[8]

- **Synchronization of means and horizontal escalation.** The upper left corner of the figure lists the diverse set of means used by hybrid warfare actors, organized into color-coded MPECI instruments of power. The figure then locates the use of a particular means into a specific PMESII sector of the target.[9] In Figure 2's example, the graphic indicates that military means (color red) were used to target a critical function in the information sector of a target state.[10] For visual clarity, Figure 2 only shows the single military hybrid warfare event described above. For synchronization of means to be represented in this graphic, multiple events (star symbols) comprising different MPECI means (indicated by color) would need to be shown. Horizontal escalation would be represented in this graphic by showing a variety of hybrid warfare events comprised of multiple MPECI means across the different sectors of the target state.

- **Effects and non-linearity.** Figure 2 depicts effects by illustrating how a military event in the information sector can be related to an effect in the political sector which in turn can create an effect in the infrastructure sector. The graphic also identifies how first and second order effects stem from these events. Although not depicted here, a key aspect of the potential effects of hybrid warfare is 'death by a thousand cuts' caused by a series of synchronized, low-observable or unobserved events operating below the threshold of what would normally constitute 'war'. Moreover, they normally only become apparent once their cumulative and non-linear effects begin to manifest themselves.

[8] This graphic does not visually populate each political, military, economic, social, infrastructure, information (PMESII) sector with a concrete list of critical functions and vulnerabilities. In practice these will vary.

[9] For practical purposes, one might choose to display events that are either 'proven' or merely 'suspected' of being linked to a hybrid warfare attack.

[10] For instance, perhaps a television station satellite uplink station was destroyed in an unattributed explosion. Alternatively, a subtler example of military means operating in the information sector might involve the non-attributable yet credible threat of violence to a national newspaper demanding it end negative news coverage of a neighboring state.

# Applying the Analytical Framework to an empirical case study

To get a better understanding of how the Analytical Framework model works, this section applies an empirical case study of the Ukrainian Conflict (2013-2015)[11] to the framework. This document also contains more visual case studies on pages 27 to 30. These are intended to further help the reader understand the nature of hybrid warfare by applying the Analytical Framework.[12] The illustrative example in this section of the Ukrainian Conflict focuses on Russia's use of the economic spectrum of the MPECI instruments. Here, the use of gas and lending instruments allowed the Russians to create SAPs to put pressure on Ukrainian governments over the whole time period and synchronize them with other instruments of power such as military and informational.

## Critical functions and vulnerabilities

The case study identifies two types of vulnerabilities that represent enabling factors for facilitating the implementation and execution of a specific synchronized economic attack package as part of the hybrid warfare campaign.

- Vulnerabilities inherent to Ukraine.
  - Weak macroeconomic fundamentals in Ukraine.
  - High levels of foreign debt in Ukraine.
- Vulnerabilities created intentionally by Russia.
  - Gas supply and transit contracts between Russia and Ukraine.
  - Russian loan structure to Ukraine.
  - High levels of Ukrainian dependency on Russian gas.

## Synchronization of means and escalation patterns

The case study identifies two different SAPs.

- Synchronized attack package 1 (SAP 1) represents the adversarial actions undertaken by Russia and its proxies (mainly Gazprom and Gazprombank) within the Ukrainian gas domain during the conflict period.

[11] Annex C of the Baseline Assessment document (see page 2 for link).

[12] The detailed case studies are available at the link on page 2.

- Synchronized attack package 2 (SAP 2) represents adversarial actions undertaken by Russia within Ukraine's foreign debt domain during the conflict period.

During the period leading up to the conflict the Russians used a combination of political pressure and compensation in the form of cheap gas and loans via the SAPs to encourage president Yanukovych to abandon the signing of the European Union (EU)-Ukraine Association Agreement.  As the conflict evolved and the strategic environment changed, Russia started using different MPECI instruments and adapted the SAPs accordingly to synchronize the effort through different patterns of vertical and horizontal escalation and de-escalation.[13]

With the identified vulnerabilities still in place, Russia was able to use both coercive and escalatory, and compensatory and de-escalatory tools – offering and cancelling loans, and increasing and decreasing gas prices and supply – to pressure the new pro-Western government in Kiev.  They reduced prices while keeping the unfavorable indexation formula unchanged and restored gas supplies while filing a multibillion-dollar claim to international arbitration.  This was done in synchronization with other tools such as military and informational instruments.  Escalation in military force was, for instance, synchronized with compensatory or coercive use of the SAPs – offering cheap supply of gas and loans or threatening with supply shortage and debt repayment – prior to the Minsk agreements.

Ambiguity played an important role in the conflict. Ukraine was generally aware of the risks associated with the energy and economic deals with Russia. However, it was unable to correctly grasp how the gas contracts and loan structures were designed in a premeditated fashion as baits that would lead to further strategic entrapment that would allow Russia to use them with a pure adversarial intent should the need arise.

## Effects

The effect of the political pressure, combined with the cheap gas and loans, was the abandonment of the EU-Ukraine Association Agreement by President Yanukovych.  With the benefit of hindsight, it can be said that this set off a number of non-linear effects in all of the PMESII sectors of which the Maidan protests and the eventual ousting of the President are key examples.  Perhaps the most interesting aspect of the non-linear effects resulting from Russian actions was that Moscow showed great flexibility and adaptability in capitalizing

[13] For a chronological pattern of vertical and horizontal escalation see Figure 3 in Annex C of the Baseline Assessment document at the link on page 2.

on the unpredictable events that followed the social and political chaos in Ukraine. Without speculating on Russian intentions, Moscow did capitalize on the turmoil in Ukraine to annex Crimea and adapted to the changing circumstances by refashioning their SAPs from compensatory to coercive instruments (for example, acceptance of the loan offer provides a temporary relief for Ukraine but over the medium to long term it leads to financial and political dependence).

Throughout the whole conflict period examined in this case study, the SAPs were active parts of the synchronized means that Russia used to great effect in escalating or de-escalating the conflict as they saw fit. For instance, the 'nuclear options' or maximum vertical escalation embedded within the SAPs that could have been used in the conflict remained on the table. While Moscow decided against using this option because it would likely have caused economic collapse with unpredictable and negative consequences for Russia, it is also likely that one of the effects of the embedded 'nuclear options' was a successful deterrence of Ukraine from annihilating Russian proxies with the use of conventional military forces.

## Visualizing the hybrid warfare case study

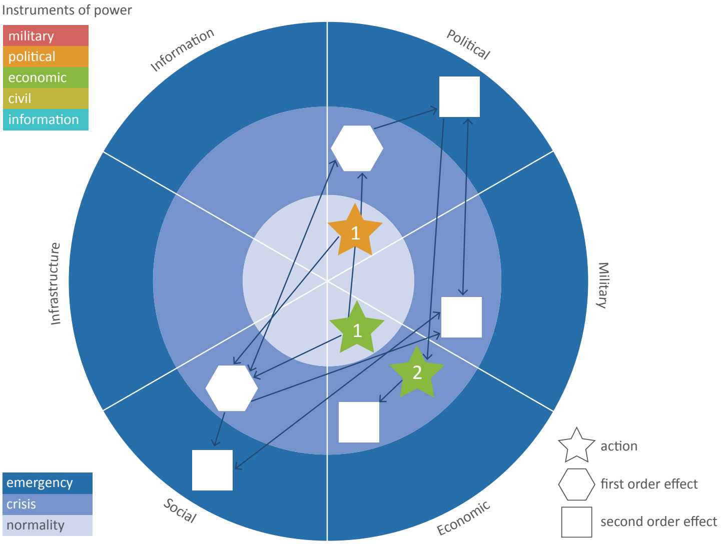


Figure 3 – Visualizing the hybrid warfare case study

Figure 3 depicts the early stages of the conflict (Phase 1: 01.10.2013 to 22.02.2014) which covers the months preceding the EU Eastern Partnership Summit in Vilnius and the Maidan protests culminating in the ousting of President Yanukovych. It shows how political pressure (action star in the political spectrum) is synchronized with the compensatory elements of the SAPs (action star in the economic spectrum). The decision to abandon EU negotiations resulted in social crisis (first order effect in the social spectrum) and a political crisis (first order effect in political spectrum) that were mutually reinforcing. The escalation of the protest, the ensuing violence (second order effect square in the military spectrum) and the eventual ousting of president Yanukovych led to social and political emergency (second order effect square in the social and political spectrum). This prompted the Russians to cancel the loan offer and demand the repayment of gas debt (action star 2 in the economic spectrum) putting further pressure on the new government in Kiev (second order effect square in the economic spectrum).

## Concluding observations

Throughout the conflict period, the Russians were active in tactically and operationally switching between escalation and de-escalation across various instruments of power. Although compensatory measures played an important role, Russia was able to keep the overall level of strategic escalation high and stable. By synchronizing various elements such as the gas supply and pricing and the loan offers, the Russians expanded the number of potential tactical combinations that could be utilized for strategic utility.

The SAPs were designed in a way that they could be simultaneously used to escalate or de-escalate and used for compensation or coercion depending on the changing circumstances of the conflict. Both SAP 1 and SAP 2 is indicative of Russia's deliberate and highly structured and flexible approach to shaping potential future conflict space. While the decisive moments of the conflict (for example, annexation of Crimea, Minsk 1 and Minsk 2) were dictated by hard military power, SAP 1 and SAP 2 likely provided escalation dominance for a limited military campaign.

While this section is only a limited outline of a very complex conflict it shows how the Analytical Framework can be used to further our understanding of how tailor-made synchronized attack packages work against specific contextual vulnerabilities in the target system. The instruments of power used by the Russians were tightly linked to their capabilities and the vulnerabilities of Ukraine, all orchestrated in escalation and/or de-escalation patterns according to their political goals. In addition, they were used in ambiguous ways, hidden from view or conducted with unclear intentions making it difficult for the Ukrainians to understand and respond until the instruments had already taken effect.

The case study shows clearly how a hybrid warfare attack in one sector has effects in different sectors, but it also shows that controlling the non-linear effects is not always possible. Importantly, this Russian hybrid warfare attack was specifically designed to the political, social, economic, informational and military context Ukraine found themselves in.

# Baselines, thresholds, and indicators

As the previous case study shows, hybrid warfare attacks focus on specific vulnerabilities of the target making them highly contextual. To respond to this threat, certain steps need to be followed.

First of all, the target needs an assessment of its critical functions and vulnerabilities. Once critical functions and vulnerabilities are identified, thresholds must be established to monitor changes in the functional status (for example, the total stress) of one’s critical functions. Thresholds help identify and define the severity of a hybrid warfare attack (or suspected attack) by pre-determining levels (for example, normality, crisis or emergency) along with the magnitude or intensity that must be exceeded to move from one status level to the next.

Specific indicators should also be built to help determine if and when a hybrid warfare action or effect is occurring. Building a baseline (for example, status normal) is a critical first step in identifying hybrid warfare activity. Without having a sense of what is normal, it is difficult to ‘see’ actions that may be part of an ambiguous hybrid warfare attack.

An attack from a hybrid warfare actor using the MPECI instruments of power may be disruptive, but not to an extent that one is able to distinguish them from normal incidents. However, if it happens many times or in other sectors simultaneously, it may cross thresholds due to the fact that synchronized efforts can lead to cumulative and non-linear effects.

The Baseline Assessment established that hybrid warfare does not neatly fit into traditional attack-phase thinking. It does not necessarily evolve linearly through escalatory phases towards a strategically defined end state. Instead of operating in phases, a hybrid warfare attack evolves through simultaneous escalation and de-escalation at the tactical and operational level across the vertical and horizontal axis, flexibly exploiting and taking advantage of effects as they occur. As such, understanding a hybrid warfare attack and how to respond to it requires a near real-time monitoring of one's vulnerabilities, the capabilities and actions of a hybrid warfare actor and the possible effects attacks against the system may cause.

# Monitoring in real time

As we have seen, responding to a hybrid warfare threat requires it to be contextualized according to the specific capabilities and vulnerabilities of the target system. Since it is difficult, if not impossible, to anticipate the location of an attack, the means that will be used, or the vulnerabilities that will be exploited (or indeed even 'created') by a hybrid warfare actor, persistent monitoring of one's critical functions is necessary. Only by estimating the target system's status (critical functions and vulnerabilities) and mapping the actions taken by the hybrid warfare actor can one understand how the threat evolves and where the target system is in terms of its state (normal, crisis or emergency). This monitoring process involves identifying events as potential risks to one's critical functions, possible attempts to exploit specific vulnerabilities, and then 'connecting the dots' which enables the target to identify, react, respond and ultimately counter a hybrid warfare attack.

Figures 4a and 4b (time series 1 and 2) are illustrations of how a hybrid warfare attack may evolve over time. It does not depict the instruments used, but rather where the hybrid warfare events are located within the target system (red) and where the effects are felt (blue). In this visualization, the blue indicates the level of stress on the state/system as a whole. This also depicts how near real-time monitoring may function.

In time series 1 (Figure 4a), we see an attack located primarily in the infrastructural sector indicated by the red moving to the outer ring. The effects of this attack are felt in the political, military and social sectors (blue). The effects are most strongly felt in the social sector as indicated by the blue moving to the outer ring of that sector. In this times series example, we can see how a hypothetical hybrid warfare attack on a power grid creates social unrest, increases internal political friction, and leads to military deployments adding to overall societal stress.

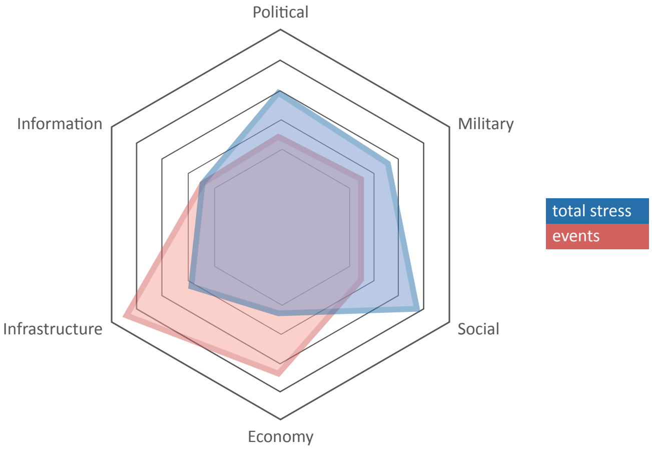


Figure 4a – Time series 1

In time series 2 (Figure 4b) we can see how the attacker followed up their attack on the infrastructure sector with attacks in the information and economic sectors (red). While the defender was able to mitigate some of the effects in the military sector, the synchronized means by the attacker has resulted in severe effects in the infrastructure, political and social sectors (blue). Finally, the hybrid warfare attacker initiates an information campaign that further destabilizes the target's government. The hybrid warfare attacker synchronizes this with economic attacks that increased pressure in the infrastructure and social sectors.

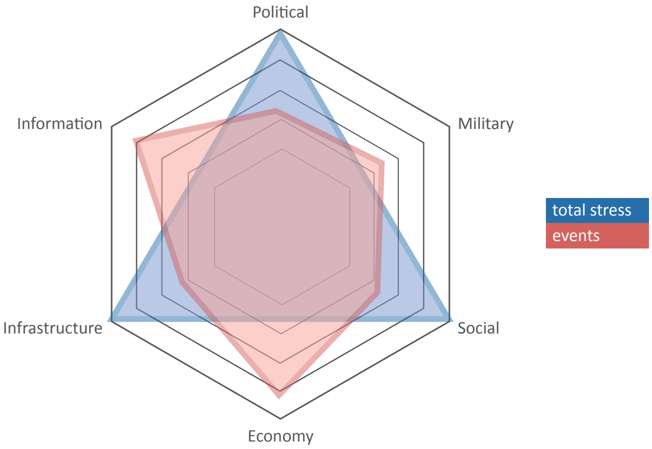
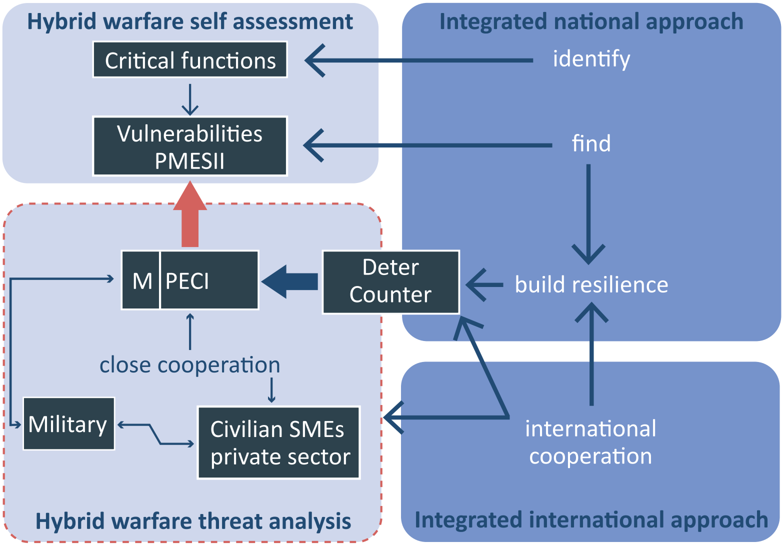


Figure 4b – Time series 2

This time series depiction of how a hybrid warfare attack might occur does not follow a linear phase model, but rather tactically and operationally escalates and de-escalates different MPECI instruments simultaneously while escalating the conflict altogether.[14] In time series 2, the attack on the infrastructure is de-escalated while the attacker shifts its focus to create hybrid warfare events in the informational and economic sector increasing the overall stress level on the target.

# Recommendations

A series of recommendations for future countering hybrid warfare efforts logically flows from the above analysis. These are visualized in Figure 5 below.


Hybrid warfare self assessment
Critical functions
Vulnerabilities PMESII
Integrated national approach
identify
find
build resilience
M
PECI
Deter Counter
close cooperation
Military
Civilian SMEs private sector
Hybrid warfare threat analysis
international cooperation
Integrated international approach

M – military
PECI – political, economic, civil, international
PMESII – political, military, economic, social, information, infrastructure
SME – subject matter expert

Figure 5 – Visual recommendations

[14] Of course, it is important to keep in mind that any attack may also develop in a linear fashion, and escalation may occur across sectors without de-escalating pressure at the original points of attack. We only wish to highlight that a hybrid warfare adversary may simultaneously escalate and de-escalate a conflict with various MPECI tools targeting different sectors. For instance, this tactic may be used to spoil multinational political coalition building against the hybrid warfare attacker.

Hybrid warfare's tailored targeting of its adversary's entire PMESII spectrum logically drives a requirement for states to conduct a hybrid warfare self-assessment to identify critical functions and find vulnerabilities (upper left box). This process does not replace traditional threat analysis. Rather, national self-assessment supplements efforts to understand the hybrid warfare threat across each of the MPECI tools that are available. The traditional threat analysis is supplemented by a hybrid warfare threat analysis (lower left box) in which the military focuses on the 'M' (military) hybrid warfare threat, while civilian subject matter experts and the private sector, in close cooperation, assist with non-traditional threat analysis dealing with political, economic, civil, informational (PECI) hybrid warfare tools. The red arrow indicates how hybrid warfare threat analysts should attempt to think of how a specific hybrid warfare actor might tailor attacks to different vulnerabilities of intended targets across the PMESII spectrum.

Crucially, this analysis must consider how these means of attack may be formed into a synchronized attack package tailored to the specific vulnerabilities of its target. Together, this process must be part of an integrated national approach coordinating whole of government, military and private sector expertise to ensure comprehensiveness (upper right box). In turn, this integrated approach should be institutionalized in an intergovernmental coordination body (for example, the Executive Counter-Hybrid Warfare Steering Committee) responsible for monitoring changes in the situation and evaluating their effects.

Institutionalizing a process to collect and disseminate threat and vulnerability information to the appropriate parties will enhance hybrid warfare early warning efforts, assist resiliency efforts, and may even have a deterrent effect as the conditions of possibility may be closed off for the attacker. Finally, in principle, these efforts should be replicated at the international and multinational levels (lower right box) to enhance counter-hybrid warfare efforts.

This analysis leads us to make the following policy recommendations.

- Hybrid warfare is designed to exploit national vulnerabilities across the political, military, economic, social, informational and infrastructure (PMESII) spectrum. Therefore as a minimum national governments should conduct a self-assessment of critical functions and vulnerabilities across all sectors, and maintain it regularly.

- Hybrid warfare uses coordinated military, political, economic, civilian and informational (MPECI) instruments of power that extend far beyond the military realm. National efforts should enhance traditional threat assessment activity to include non-conventional political, economic, civil, international (PECI) tools and capabilities. Crucially, this analysis must consider how these means of attack may be formed into a synchronized attack package tailored to the specific vulnerabilities of its target.

- Hybrid warfare is synchronized and systematic – the response should be too. National governments should establish and embed a process to lead and coordinate a national approach of self-assessment and threat analysis. This process should direct comprehensive cross-government efforts to understand, detect and respond to hybrid threats.

- Hybrid threats are an international issue – the response should be to. National governments should coordinate a coherent approach amongst themselves to understand, detect and respond to hybrid warfare to their collective interests. Multinational frameworks – preferably using existing institutions and processes – should be developed to facilitate cooperation and collaboration across borders.

# Conclusion

Hybrid warfare involves the synchronized use of military and non-military means against specific vulnerabilities to create effects against its opponent. Its instruments can be ratcheted up and down simultaneously, using different tools against different targets, across the whole of society. In this respect, hybrid warfare expands the battlefield. It also creatively exploits our cognitive predisposition to emphasize the military instrument of power, allowing opponents to leverage non-military ((M)PECI) means against a wider set of unconventional targets. This, in turn, allows hybrid warfare actors, at least initially, to operate ambiguously below the target's thresholds of detection and response. In practice, this can make identifying the starting point of hybrid warfare very difficult. Moreover, it increases the possibility of a hybrid warfare actor inflicting significant damage on its opponent before that opponent can respond to, or possibly even detect, a hybrid warfare attack.

This strong and fluid element of ambiguity within hybrid warfare adds a new dimension to how coercion, aggression, conflict and war are to be understood. In this respect, new geostrategic contexts, new applications of technologies, and new organizational forms suggest the likelihood that this form of warfare will persist and continue to evolve into the future. The Analytical Framework model developed here provides a practical guide for understanding and countering this hybrid warfare threat at the national and multinational levels.

# Applying the Analytical Framework to the case studies

This final section applies the Analytical Framework to the other case studies carried out under this project. The detailed case studies are available at the link on page 2. What is replicated here is intended to help the reader understand the nature of hybrid warfare. The examples are not exhaustive attempts to visualize every detail of each case study. Instead, they use a small selection of the data from the case studies to show how the Analytical Framework can help depict constituent parts of a hybrid attack.

# Case study: ISIL in Syria 2012 to 2014

## Overview

ISIL takes advantage of the turmoil in Iraq and Syria to establish a territorial and political foothold in the region. This case study highlights some of ISIL's actions over the period 2012-2014 to demonstrate a hybrid approach to achieving political goals by a non-state actor.

## Vulnerabilities

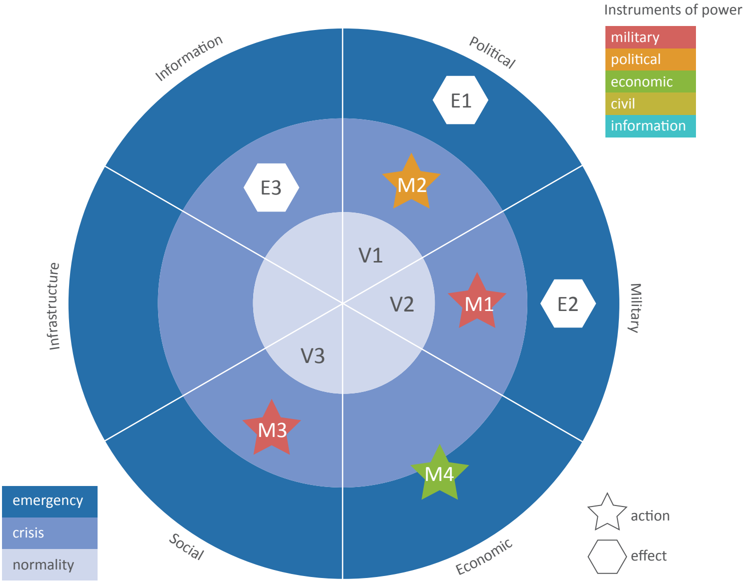
V1 – Syrian war
V2 – power vacuum in North-East Syria
V3 – existing sectarian and ethnic divisions

## Means

M1 – military training camps established
M2 – co-option of tribes in North-East Syria
M3 – extermination of tribes in North-East Syria
M4 – support to Assad (oil and electricity, for example)

## Effects

E1 – caliphate established
E2 – mumber of ISIL fighters increased significantly (to around 20-30,000)
E3 – early achievements advertised through social media



# Case study: Russia and Ukraine, phase one

## Overview

Russia takes action to prevent Ukraine's economic and political assimilation into the European Union (EU). This case study highlights examples of a state actor's use of economic and political levers to demonstrate a hybrid approach to achieving political goals.

## Vulnerabilities

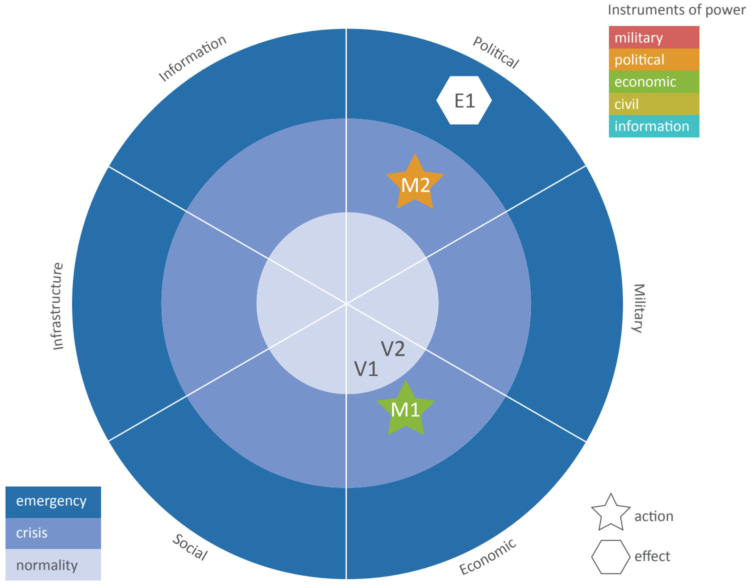
V1 – Ukrainian reliance on Russian gas
V2 – Ukrainian debt to Russia

## Means

M1 – control of Ukrainian gas supply
M2 – pressure on Yanukovych to abandon EU negotiations

## Effects

E1 – negotiations grind to a halt in November/December 2014



# Case study: Russian and Ukraine, phase two

## Overview

Following the removal of Yanukovch from power and the Maidan protests in early 2014-2015, Russia takes action that results in the *de facto* annexation of Crimea. This case study highlights examples of a state actor's use of synchronized means to demonstrate a hybrid approach to achieving political goals.

## Vulnerabilities

V1 – political leadership in Ukraine

V2 – social cohesion in Ukraine

## Means

M1 – Russian military actions in Crimea

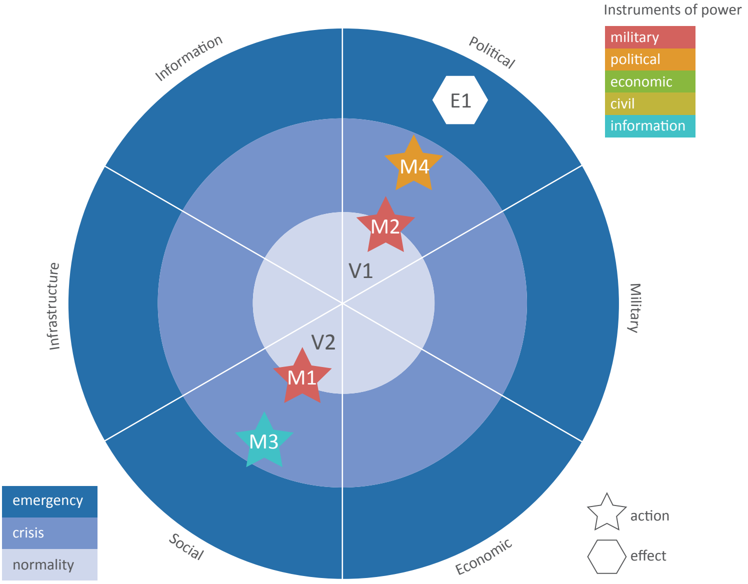
M2 – heavy fighting in Donetsk in September and January

M3 – digital propaganda and disinformation

M4 – local referendum

## Effects

E1 – annexation of Crimea; Minsk Accords



# Case study: Iran's hybrid warfare in Syria

## Overview

Iran's involvement in the ongoing conflict in Syria highlights examples of a state actor's use of synchronized means to demonstrate a hybrid approach to achieving political goals.

## Vulnerabilities

V1 – deep ethnic and sectarian divisions in Syrian society

V2 – Syrian opposition disadvantages in military (heavy weapons, command and control) and information (cyber).

## Means

M1 – Iranian military action in Syria through regular armed forces, Islamic Revolutionary Guard Corps, Hezbollah and other foreign Shia militia

M2 – financial and material aid to the Syrian regime

M3 – digital propaganda

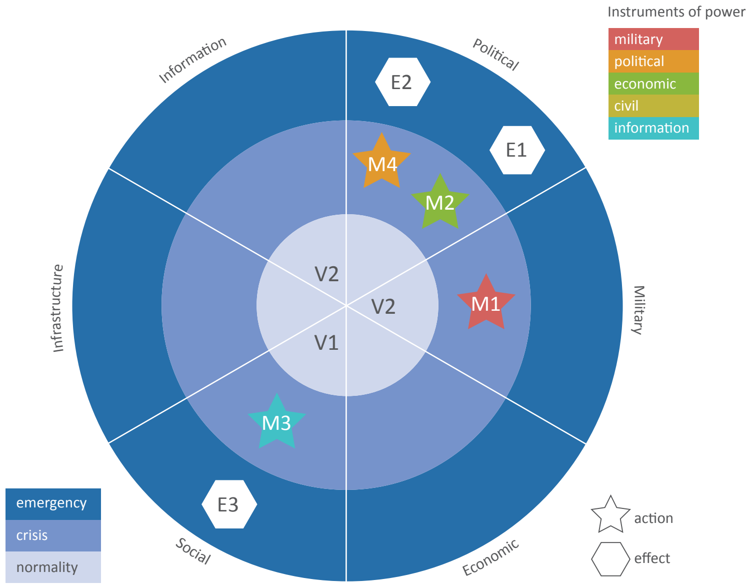
M4 – influence through pan-Shia clergy networks

## Effects

E1 – Syrian regime retains a strong position on the ground

E2 – Western and Arab actors deterred from intervening decisively

E3 – radicalization of Sunni armed opposition in Syria (ISIL and al-Qaeda affiliates)



# Glossary

Ambiguity is defined here as hostile actions that are difficult for a state to identify attribute or publicly define as coercive uses of force.[15] Ambiguity is used to complicate or undermine the decision-making processes of the opponent. It is tailored to make any type of response difficult. In military terms, it is designed to fall below the threshold of war and to delegitimize or render irrational the ability to respond with the use of military force.

Baseline is a reference point to allow for the identification of indicators and events as well as measurement of variation away from that reference point. Establishing a baseline is a key part of the hybrid warfare self-assessment process.

Critical functions are activities or operations distributed across the political, military, economic, social, information, infrastructure (PMESII) spectrum the discontinuance of which would lead to the disruption of services that a working system (for example, a state, its society, or a subsection thereof) depends on. Critical functions can be broken down into a combination of actors (for example, individuals or organizations), infrastructures (for example, 'critical' national power grids) and processes (for example, legal/jurisdictional, technical, political).

Effects are a change of state of an entity as the result of actions against specific vulnerabilities of a target system.

Horizontal escalation is the applied combination of multiple military, political, economic, civil, informational (MPECI) means.

Hybrid warfare threat analysis is an analysis/process designed to account for the all MPECI instruments of a hybrid warfare threat. While the military focuses on the M (military), civilian subject matter experts and private sector are brought in to assist non-traditional threat analysis of PECI (political, economic, civil, informational) hybrid warfare tools. The key to the success of this process is understanding how specific hybrid warfare actors tailor attacks to specific vulnerabilities of intended targets across the PMESII spectrum.

Hybrid warfare self-assessment is a continuous national process to identify critical functions and find vulnerabilities within the PMESII spectrum.

[15] Andrew Mumford and Jack McDonald, *Ambiguous Warfare.* Report produced for the Development, Concepts and Doctrine Centre, October 2014.

Indicators are measurable variables necessary to clearly and sufficiently identify/describe/represent/monitor a phenomenon in relation to a specific baseline.

Instruments of power are elements of the MPECI environment. When these elements are 'weaponized' the instruments of power can become tools of attack.

Non-linearity refers to unanticipated effects of hybrid warfare attacks that are not causally linear. They are the result of synergistic interactions of hybrid warfare attacks in which the whole is greater than the sum of their parts. Non-linear effects cannot always be predicted by the attacker or defender.

Synchronization of means is the ability of a hybrid warfare actor to effectively coordinate the instruments of power (MPECI) to achieve the desired effects in both horizontal and vertical ways.

Synchronized attack packages (SAPs) are specific MPECI means that are synchronized and tailored to specific vulnerabilities that are used in a hybrid warfare attack.

Threshold is determining the magnitude or the intensity of a functional status (for example, the 'stress level') of one's critical functions to be exceeded to achieve a specific status (for example, normal or crisis).

Vertical escalation is the intensified use of one specific means.

Vulnerabilities are personnel, activities, resources or processes within a potential target that are susceptible of being exploited or created by a potential adversary.

MCDC

Multinational Capability Development Campaign

For more information, contact: MCDCsecretariat@apan.org