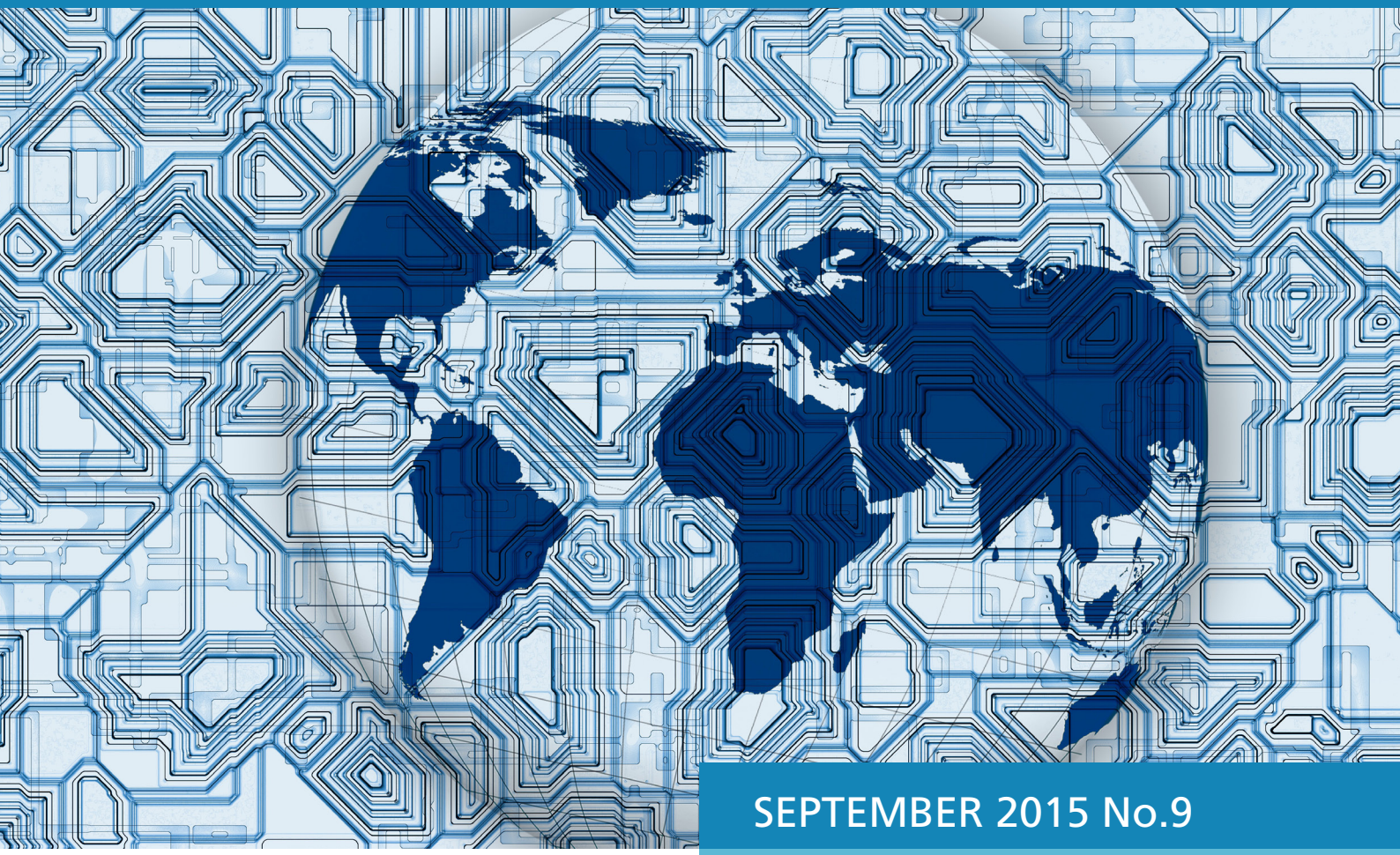
GCSP
Geneva Centre for Security Policy
Where knowledge meets experience



SEPTEMBER 2015 No.9

STRATEGIC SECURITY ANALYSIS

How can Societies be Defended against Hybrid Threats?

by Aapo Cederberg and Pasi Eronen

How can Societies be Defended against Hybrid Threats?

Hybrid threats, hybrid operations and hybrid warfare have been widely discussed among political decision makers and security policy analysts, particularly during the past couple of years.

The latest round of discussions was sparked by Russia's integrated use of military and other means in the Crimean peninsula during the early phases of the Ukraine crisis.[1]

While the descriptive and definitive sides of hybrid threats, operations, and warfare have been widely covered, there has been less discussion on what enables countries to engage in hybrid warfare and how to organise robust national defences to cope with hybrid threats.

This policy paper's main contributions lie in introducing a framework to evaluate the strategic underpinnings for offensive hybrid operations and in listing suggestions for organising national defences to cope with the spectrum of hybrid threats.

KEY POINTS

- Hybrid warfare intentionally blurs the distinction between the times of peace and war making it hard for the targeted countries to devise policy responses in a proper and timely manner.
- The multi-pronged hybrid threat demands that defence planners engage all parts of society in defensive efforts. Intergovernmental or interagency efforts are not enough anymore.
- The comprehensive defence approach requires a patient build-up of national capabilities. In the short term, shortcomings can be overcome by utilising the capabilities and capacity-building efforts of one's allies.

1 Michael Kofman and Matthew Rojansky, "A Closer Look at Russia's 'Hybrid War,'" *Kennan Cable*, no. 7 (April 2015), http://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf.

1 Hybrid warfare - mobilisation of all national means to achieve political goals

In this paper, hybrid warfare is seen as a concept that is a Western attempt to categorise what was witnessed in Ukraine. The often cited Russian "Gerasimov doctrine" describes modern warfare as joint operations utilising a mix of military and nonmilitary means to achieve political goals, and taking full advantage of the intentionally blurred line between war and peace.[2] As has been pointed out earlier, in the history of warfare we have seen similar activities under various terms, including for example non-linear operations, low-intensity conflict, full spectrum conflict, political warfare, unconventional warfare, irregular warfare, asymmetric warfare, and unrestricted warfare.[3] Nevertheless, it is important to keep in mind that the art of war is developing all the time and we often encounter new mutations or rehashes of previously well-known doctrinal approaches.

2 Hybrid warfare in a nutshell

It is our view that in regard to hybrid warfare (Fig. 1), the constant exploitation of identified asymmetries throughout all phases of warfare, including the nonviolent phases, is one of the defining features. Secondly, these asymmetries are exploited typically in combination with an element of surprise and an application of diversion and deception tactics. The third defining feature is linked to the temporal aspect of the conflict. In hybrid warfare, it is by no means

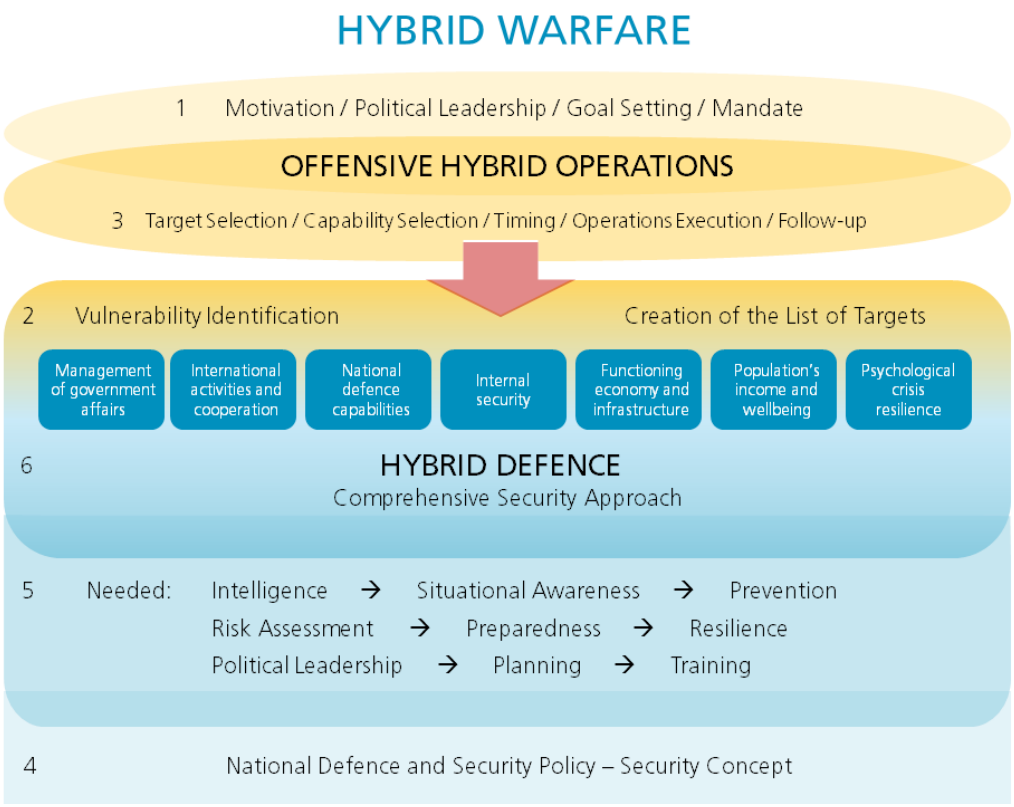


Figure 1. High level view on hybrid warfare from offensive and defensive perspectives

2 Janis Berzinš, *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy* (Center for Security and Strategic Research, National Defence Academy of Latvia, April 2014); Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows*, July 6, 2014, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

3 Frank Hoffman, "On Not-so-New Warfare: Political Warfare vs Hybrid Threats," War on the Rocks, July 28, 2014, http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/; Oscar Jonsson and Robert Seely, "Russian Full-Spectrum Conflict: An Appraisal After Ukraine," *The Journal of Slavic Military Studies* 28, no. 1 (2015): 1–22.

necessary to have a decisive quick win over the adversary, but the level of escalation can ebb and flow over a longer period time. A more active phase of a conflict can be followed by a time of frozen conflict, which can serve to reach the original political goals and thus "win".

From the operational perspective, hybrid operations can be described as including a combination of two or more violent or nonviolent state means or power projection capabilities to achieve the desired political end state. These include, but are not limited to, political and economic tools, information warfare, use or threat of military force, cyber attacks, and engaging in special operations.[4] While combining violent and nonviolent means to achieve goals is an age-old phenomena, the flexible and swift coordination of the use of various means and the way that targeting is done can be considered to be novel features. The key targets for hybrid operations are the identified vulnerabilities or weaknesses in the target country. These vulnerabilities can be identified from any of the vital parts of a society.

In order for hybrid operations to be successful, it requires critical preconditions and preparations. First of all, there needs to be strong political leadership in place to mandate the hybrid operations combined with both the will and ability to dedicate a wide array of resources for the operations on short notice, as well as in the longer run. Secondly, an effective and wide-ranging intelligence apparatus is needed to scan the target countries and create a list of identified vulnerabilities. The list of identified vulnerabilities, or the list of targets, is based on the acquired knowledge of the key vulnerabilities and weaknesses that exist in the society of the target country. Third critical precondition that is often associated with hybrid operations is the information campaign preceding the hybrid operations.[5] These information campaigns are aimed at raising support for the operations both internally and in the target country, which was seen in the case of the "polite green men" in Crimea.[6] Information operations will also continue to take place during and after the active phase of the hybrid operation. Political support, the application of intelligence apparatus, and information operations are all crucial throughout the preparations, execution, and follow-up phases of hybrid operations.

It has been argued that hybrid warfare is in its essence winning, or achieving the set goals, with little or no fighting.[7] To build upon this idea, we say that in hybrid war it is nearly impossible to say when the actual fighting, or organised violence that is war in its classic form begins. One of the core ideas of hybrid warfare is that it intentionally blurs the distinctions between the neatly separated Western categories of war and peace, and civilian and military operations. This blurring is achieved by utilising a wide variety of means, both violent and nonviolent, military and civilian, in a carefully planned way without unnecessarily breaching the threshold of war, even if the level of escalation varies.

As hybrid warfare is based on tapping into a wide array of society's resources and mobilising them for political purposes, the Western liberal democracies are limited in their capabilities to wage hybrid war to its maximum, particularly during a time of perceived peace. Developed and globally integrated autocratic societies can be considered to be better positioned to engage in hybrid warfare. The autocratic regime type allows quick, centralised decision-making that is less limited by the normal checks and balances, and which has better access to natural resources. Development and global integration widens the set of available instruments and offers avenues to apply the tools against their targets.

3 Offensive hybrid operations

As was briefly mentioned earlier, an offensive hybrid operation can be divided to three phases: preparations, operations, and follow-up. While hybrid operations are always carefully tailored according to their targets, the pre-conditions and preparations behind the operations stay the same.

1. Strong political leadership is needed, as it helps to set goals and provides the mandate

4 Keir Giles et al., *The Russian Challenge* (Chatham House, June 2015), chap. 6.

5 András Rácz, *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*, FIIA Report (The Finnish Institute of International Affairs, June 16, 2015).

6 Keir Giles, "Western Media Must Get Creative in Infowar," *The Moscow Times*, August 4, 2015, http://www.themoscowtimes.com/opinion/article/western-media-must-get-creative-in-infowar/527000.html.

7 Fiona Hill, "Hybrid War: The Real Reason Fighting Stopped in Ukraine – for Now," *Reuters*, February 26, 2015, http://blogs.reuters.com/great-debate/2015/02/26/hybrid-war-the-real-reason-fighting-stopped-in-ukraine-for-now/.

to the operations. Political leadership is also a necessity both to enable quickly executable snap operations and to keep longer operations running for a potentially undecided length of time.

2. There needs to be a set of existing state controlled instruments or capabilities available that can be utilised to carry out hybrid operations. For example, a strong military force may be needed to back the ongoing nonviolent operations and to create deterrence against potential backlash. The instruments available need to match with the identified vulnerabilities in the target state.

3. For hybrid operations to be successful and well orchestrated, tight control and coordination over all state and some private means is necessary as hybrid operations combine a variety of instruments in a joint fashion.

4. A strong intelligence apparatus and up-to-date situational awareness are necessary to lead hybrid operations effectively and to enable swift changes in the operations' outlook and set of instruments in use to stay one step ahead of the defender.
5. The element of surprise is key to success, which is achieved by orchestrating the use of various instruments in an unexpected way, and by utilising diversion and deception tactics.

6. Lastly, strong political follow-up is needed to protect the achieved end state and the gains made.

Hybrid operations are based on utilising identified asymmetries to make the operations successful by pitting one's own strengths against the targets' known weaknesses. For example, a weak government in a target country may succumb to political pressure, or even fall with additional help from covert destabilisation operations. But the key difference that sets hybrid warfare apart is that hybrid operations take full advantage of the joint impact of several simultaneous operations or actions that take place in a sequential or concurrently orchestrated manner. The hybrid operations toolbox consists of a wide array of instruments that can be utilised for offensive purposes (Fig. 2).

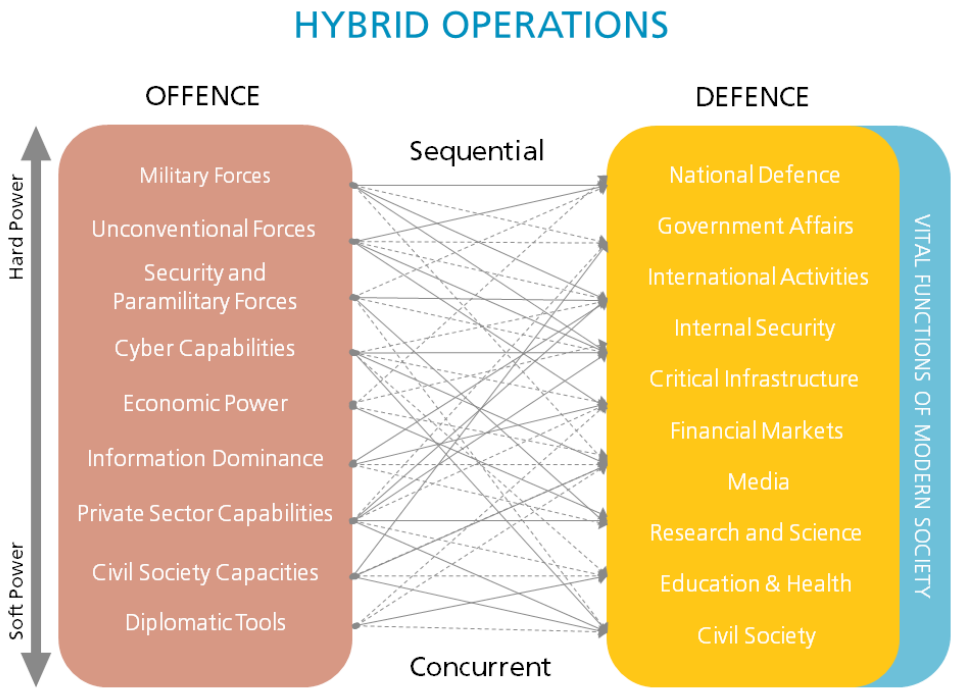


Figure 2. Offensive hybrid operations and their potential targets [8]

8 Figure has been inspired by Anton Dengg's work on the subject.

4 Hybrid defence - establishing a comprehensive defence approach

Hybrid threats are now receiving special attention in national defence planning circles. This is particularly true in countries that face a current or potential adversary with the necessary capabilities to run hybrid operations. Even further attention should be placed on hybrid defence if there are major fault lines among the population that can be taken advantage of by the aggressor.[9]

Because of the very whole-of-society nature of hybrid threats, preparing for and addressing them requires strong measures. The main liberal democracies may enjoy unrivaled power in many of the areas of hybrid warfare, offensive uses included, but may lack the tools necessary to identify in a timely manner threats that nimbly cross the neat categories and carefully guarded bureaucratic silos. Smaller countries with less power may have potential in some of the areas of hybrid warfare, such as cyber, information warfare, and key areas of the economy like energy, but are seldom able to engage in hybrid warfare alone. This is due to the fact that smaller countries often lack the political agenda, the wide intelligence gathering apparatus to acquire a list of potential targets, and the capability to flexibly utilise a wide array of hybrid warfare instruments for successful operations.

However, regardless of their size, all countries can shore up their defences against hybrid threats. The key in this is a comprehensive security approach, which aims at intersocietal security planning instead of settling with a classic intergovernmental approach (Fig. 1). The comprehensive security approach demands political leadership, as the whole society should be engaged in defensive efforts. This approach needs to be combined with clearheaded vulnerability analysis to understand the potential pressure points in one's own society, access to reliable intelligence, and robust counterintelligence efforts.

5 Organising hybrid defences

While strong and developed autocratic nations may have an advantage on the offensive side of hybrid operations, all countries regardless of their position in the international order have an opportunity to organise their defences against hybrid threats. A credible defensive posture against hybrid threats cannot be based solely on military forces and other security providers, because the targets can be located anywhere in society depending on each country's individual vulnerabilities (Fig. 2). Thus, hybrid defences must be built as a joint action of all stakeholders in society, including also representation from civil society and the private sector. This model is called acomprehensive security approach.

The idea behind a comprehensive security approach is that society's security does not rest on the prowess of traditional security providers such as police and military alone, but all the key sectors of society have been included in the security planning and implementation process. This whole-of-society aspect of a comprehensive security approach makes the political leadership particularly important. Including a wide range of society's players in the security planning and implementation process aims both at increasing capabilities to respond to a wide range of threats (such as cyber) that cross sectoral boundaries, but also to secure the vital functions of society that usually demand tight collaboration between several sectors. This efficient collaboration allows wide and efficient mobilisation of society's resources.

In order for collaboration between various parts of society to work there needs to be a shared understanding in the form of a security concept or strategy and administrative structures in place. The written and commonly agreed upon security concept ties all the parties together to tackle the common challenge, while the administrative structures, like the Security Committee in Finland,[10] brings the parties physically together for an exchange of information and establishes the capability to lead the distributed response to the threats.

For these structures to work in the anticipated manner, it is of utmost importance to have

9 Peter Pomerantsev and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money* (The Institute of Modern Russia, November 2014).

10 For a closer look at the Finnish Comprehensive Security Approach, have a look at the additional information supplied in the case study at the end.

shared situational awareness. Situational awareness supports understanding the current situation, enables warning of the adversary's operations before they are carried out, and helps to formulate an appropriate response to the unfolding situation. Reliable situational awareness demands the active collection of intelligence both from open and closed sources. Moreover, organising defences demands trustworthy intelligence and high-quality analysis. Planning for hybrid defence needs to be based on an understanding of the motivations and political goals guiding the adversary's actions and identifying the possible targets for the adversary's hybrid operations. In other words, what should be defended and for what reason?

The possible targets are the vital functions of the society and the vulnerabilities and weaknesses residing in them. As it was covered earlier, the adversary's goal is to figure out the vulnerabilities; where there are greatest asymmetries available, which targets are easiest to attack, and how the attacks should be orchestrated so that maximum impact could be achieved. This leads to a need to conduct a national threat and risk assessment to define the vital functions of the society and to find out the vulnerabilities in them. The national threat and risk assessment should also include the critical infrastructure and key resources with their vulnerabilities. National threat and risk assessment also helps identifying a relevant set of threat scenarios that are used in support of defence preparations across the society.

Related to intelligence, it is also necessary to have well-resourced counterintelligence, as it is the first line of defence against a hybrid threat. In order to be efficient, hybrid operations demand a detailed and up-to-date understanding of the target country's vulnerabilities. While a lot of information is available from open sources, some information still needs to collected from human sources and classified systems. Furthermore, intelligence operators can engage in active measures within the target country, such as corrupting key officials or damaging infrastructure. Counterintelligence needs to be able to prevent access to the most crucial information and prevent operators from conducting their tasks successfully. At the time of crisis, the goal of counterintelligence is to deny the aggressor access to up-to-date information on the status and success of their ongoing operations.

To single out a threat, modern societies are more and more dependent on digital services and critical infrastructures, which at the same time are vulnerable to cyber exploitation.[11] The interdependencies of these key functions of society offer interesting avenues for offensive hybrid operations. An example of this is social media, where "troll factories" consistently challenge the narratives in national and global media.[12] We have witnessed an improvement in the quality and quantity of disinformation, which has unfortunately been successful in having an impact in the opinions of both decision-makers and those of ordinary citizens. For these reasons, cyber and media power can be considered to be the spearheads of hybrid operations and critical challenges for the hybrid defence.

It should also be remembered that defensive efforts can have a strong international component. International collaboration offers direct political, economic and military support, but also helps in covering some of the missing national capabilities and support in developing capacities in areas that have fallen behind. Similarly to mobilising national resources efficiently, international collaboration allows for the unification of dispersed national resources under the wider international umbrella of a political agenda and leads to an improved defensive posture for all those included.

There are also more active, offensive defence measures that can be taken against the aggressor. These measures, such as changes in the placement of military forces, applying economic coercion tools, targeted strategic communications, and political operations aim both at signalling the aggressor and denying its ability to use its existing tool set for hybrid operations.

To conclude, the key questions that should be taken into account when devising national defences against hybrid threats include:

- What are the key national vulnerabilities that one should pay particular attention to? How could an adversary take advantage of those vulnerabilities? In other words, what are the relevant threat scenarios?
- Are all the necessary sectors of society engaged in the defensive efforts and have they been adequately prepared to act in their respective sectors against the perceived threats?

11 Aapo Cederberg, *Future Challenges in Cyberspace* (Geneva Centre for Security Policy, April 2015).

12 Adrian Chen, "The Agency," *The New York Times Magazine*, June 2, 2015, http://www.nytimes.com/2015/06/07/magazine/the-agency.html.

- Is there a shared understanding of the situation in times of both peace and crisis that can be utilised to lead activities in various sectors of the society?
- Are the intelligence activities providing early warning, ongoing situational awareness and analysis? Are core functions actively defended against foreign penetration and malicious activities?
- What kind of support can be found from the international community to support one's own defensive efforts? What capabilities can be offered to support others facing similar threats?

6 Concluding remarks

While parts of hybrid warfare can be seen as novel developments upon previously well-known concepts of war, to some degree we can see the return of traditional, all-consuming war. This can be seen as a clear step aside from the limited, neatly contained technowars fought in places far away from our societies that have been lulled into continuous peace.

If we are willing to accept that the fighting is going on perpetually and that the frontlines may cover the whole of society, the defender must be able to put forward a comprehensive defence solution. This should allow an agile and distributed response to multi-pronged hybrid threats. Through this kind of comprehensive security approach, the defender can build a more resilient society able to face the threats.

Building societal resilience is the only assured way of keeping at least some of the home-field advantage because the aggressor will try to build-up and utilise the effect of surprise. This, however, is not an easy task. It requires a long term plan and dedication to implementation.

First, a strong political mandate and security concept need to be in place. Second, planning, awareness building, and education are needed. Third, the key stakeholders in various parts of the society must share a common situational awareness, threat and risk assessment, and planning and training processes.

Building a more resilient society should not be viewed only as an extra burden for already economically struggling Western societies; it is also a great opportunity. The structures that allow a society to respond in an agile manner to hybrid threats also support better understanding and coping with the complex underlying interrelations that make our modern societies fragile. These defensive structures also help to make our societies more functional, as decision-making processes become more transparent and inclusive.

Case study: Hybrid defence in Finland

The preparedness arrangements in Finland offer a living example of the comprehensive security approach. Society's vital functions are secured through collaboration between authorities, the business community, civil society organisations and individual citizens.

This model has been a key element in the work for improving preparedness at the governmental and societal level. The Finnish security concept involves all stakeholders within society because hybrid attacks do not respect any artificial boundaries between sectors, nor do they separate ordinary citizens from governmental or business entities.

As the cooperation also involves companies and civil society organisations, it is important to emphasise intersocietal cooperation, rather than intergovernmental or interagency cooperation. Finnish companies have been building a safer environment even on a voluntary basis. Cooperation is more than just doing business on commercial terms. There are more than 2,000 companies voluntarily participating in the network organisation for National Emergency Supply Agency, an organisation supporting national preparedness.[1]

The Security Strategy for Society forms the conceptual backbone of hybrid defence.[2] Nevertheless, the strategy documents are not helpful without efficient implementation. In the Finnish security concept, ministries and agencies are responsible for implementing security strategies within their respective administrative branches. The responsible authorities carry out the tasks related to hybrid security and the arrangements pertaining to the security and development of supply. The implementation plan outlines how the responsibilities are shared.

The annual review by the Security Committee, where all the Permanent Secretaries of Ministries and heads of the most important security offices are brought together, ensures that the strategies are up-to-date and measure the progress made. By providing the strategy and implementation plan and monitoring its assessment, the Security Committee gives strong impetus to all the ministries.

To give a couple of concrete examples of activities where Finland has improved its defences against hybrid threats: the state works to improve the national situational awareness in cyberspace and is an active partner in regional defence initiatives and exercises. The government has also established the National Cyber Security Centre. The computer emergency response team (GOV-CERT) and 24/7 functioning of the public sector are being created and improved. Authorities and resources for the police and military, intelligence included, working in the cyber domain are thoroughly looked at. In regard to regional partnerships, Finnish experts have been sent to NATO's Centers of Excellence in Tallinn and Riga and all branches of the Finnish Defence Forces have taken part in the military exercises organised in the greater Baltic Sea region.

1 A closer look at security of supply in Finland can be found from NESA's website: http://www.nesa.fi/.

2 For more information, see: http://www.yhteiskunnanturvallisuus.fi/en.

About the authors

Aapo Cederberg is an Associate Fellow in the Emerging Security Challenges Programme at the GCSP and also a retired colonel from the Finnish Armed Forces. He was previously the Secretary General for the Finnish Security Committee and prior to that was the Head of Strategic Planning in the Ministry of Defence.
Twitter: @ace_aapo

Pasi Eronen is a project researcher for the Foundation for Defense of Democracies, focusing on economic power projection and cyber warfare. He was previously an Executive-in-Residence at the GCSP.
Twitter: @pasieronen

Bibliography

Berzinš, Janis. *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*. Center for Security and Strategic Research, National Defence Academy of Latvia, April 2014.

Cederberg, Aapo. *Future Challenges in Cyberspace*. Geneva Centre for Security Policy, April 2015.

Chen, Adrian. "The Agency." *The New York Times Magazine*, June 2, 2015. http://www.nytimes.com/2015/06/07/magazine/the-agency.html.

Galeotti, Mark. "The 'Gerasimov Doctrine' and Russian Non-Linear War." *In Moscow's Shadows*, July 6, 2014. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

Giles, Keir. "Western Media Must Get Creative in Infowar." *The Moscow Times*, August 4, 2015. http://www.themoscowtimes.com/opinion/article/western-media-must-get-creative-in-infowar/527000.html.

Giles, Keir, Philip Hanson, Roderic Lyne, James Nixey, James Sherr, and Andrew Wood. *The Russian Challenge*. Chatham House, June 2015.

Hill, Fiona. "Hybrid War: The Real Reason Fighting Stopped in Ukraine – for Now." *Reuters*, February 26, 2015. http://blogs.reuters.com/great-debate/2015/02/26/hybrid-war-the-real-reason-fighting-stopped-in-ukraine-for-now/.

Hoffman, Frank. "On Not-so-New Warfare: Political Warfare vs Hybrid Threats." *War on the Rocks*, July 28, 2014. http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/.

Jonsson, Oscar, and Robert Seely. "Russian Full-Spectrum Conflict: An Appraisal After Ukraine." *The Journal of Slavic Military Studies* 28, no. 1 (2015): 1–22.

Kofman, Michael, and Matthew Rojansky. "A Closer Look at Russia's 'Hybrid War.'" *Kennan Cable*, no. 7 (April 2015). http://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf.

Pomerantsev, Peter, and Michael Weiss. *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. The Institute of Modern Russia, November 2014.

Rácz, András. *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*. FIIA Report. The Finnish Institute of International Affairs, June 16, 2015.

Where knowlege meets experience

The GCSP Strategic Security Analysis series are short papers that address a current security issue. They provide background information about the theme, identify the main issues and challenges, and propose policy recommendations.

Geneva Centre for Security Policy - GCSP
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
CH-1211 Geneva 1
Tel: + 41 22 730 96 00
Fax: + 41 22 730 96 49
e-mail: info@gcsp.ch
www.gcsp.ch