Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Yuriy Danyk, Tamara Maliarchuk, Chad Briggs,
Connections QJ 16, no. 2 (2017): 5-24
https://doi.org/10.11610/Connections.16.2.01

Research Article

Hybrid War: High-tech, Information and Cyber Conflicts

Yuriy Danyk,[a] Tamara Maliarchuk,[a] and Chad Briggs[b]

[a] *Zhytomyr Military Institute of Radioelectronics "S.P. Korolyov," http://www.zvir.zt.ua*

[b] *Global INT*

Abstract: This article examines the advanced technological, information and cyber components of hybrid war and the introduction of suggested countermeasures to counter information and cyber threats and attacks. The main hypothesis of the authors is that revolutionary development and rapid implementation of technologies in innovative ways in all spheres of life facilitate and shape the basis for the transformation of theoretical and practical paradigms of war and conflict. The focus of the article is on the hybrid nature of modern conflict.

Keywords: Hybrid warfare, information operations, cyber war, innovative warfare, Ukraine.

Introduction

Analyses of geopolitical and geostrategic environments have hinted at a reformulation of both the philosophy and art of war, developments brought about from the deployment of new technologies that allow variable intensity and strategies in conflict. These new methods, when combined with traditional understandings of conflict and security, are often coined as "hybrid" warfare. This paper examines the nature of hybrid warfare in Eastern Europe, with a specific focus on the tactics and strategies employed by Russian and allied forces in Ukraine since 2014.

The concept of hybrid warfare is not particularly new, representing a combination of conventional and unconventional/irregular warfare, extending be-

yond the battlefield to encompass economic, diplomatic, information (including psychological, cyber and misinformation), and political warfare.[1] The concept is primarily based on the ability to target distant objects and processes through non-traditional military means, particularly those critical to state and military functions. As an asymmetric approach, hybrid warfare attempts to achieve large-scale consequences utilizing modest means, such as inhibiting an adversary's military operations or preventing popular political support.[2] Overall, hybrid conflicts coordinate so-called soft actions employing a more holistic strategy that varies in intensity at different stages (initiation, acute phase, solution), which seek to destabilize internal and external processes of a state. An overall objective is to disrupt the targeted state by encouraging the destabilization of the economy, frustration and disaffection of the population, splintering of minorities or aggrieved populations, creation of conditions encouraging controlled and uncontrolled migration, suppression of civil resistance, and disruption of critical infrastructure. It is aided by the selective application of intelligence capabilities, special forces' operations, conventional military forces, and irregular combatants (terrorists, criminals, militia groups, mercenaries, resistance movements, guerillas, etc.). A contemporary example of a hybrid conflict can be clearly illustrated by ongoing and recent combat actions occurring in Ukraine,[3] Georgia,[4] and, more recently, in specific European Union countries.[5]

The concepts presented here differ slightly from some portrayals of hybrid warfare in the West (West, Western World or Western Civilization are countries in Europe, North America, Australia, Israel, Japan, South Korea, etc., united by the common views and perception of some unity on key cultural, political and economic signs, highlighting them on the background of other coun-

---

1 Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Forces Quarterly* 52 (2009): 34-39.

2 Keir Giles, *The Next Phase of Russian Information Warfare* (Riga: NATO Strategic Communications Centre of Excellence, 2016), http://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles.

3 Volodymyr P. Gorbulin, Oleksandr S. Vlasiuk, Ella M. Libanova, Oleksandra M. Liashenko, *Donbas and The Crimea: The Value of Return* (Kyiv: National Institute of Strategic Studies, 2015); Michael Kofman, "Russian Hybrid Warfare and Other Dark Arts," *War on the Rocks*, March 11, 2016, http://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts (31 August 2017).

4 David J. Smith, "Russian Cyber Capabilities, Policy and Practice," *inFocus Quarterly* (Winter 2014), www.jewishpolicycenter.org/2013/12/31/russian-cyber-capabilities/ (31 August 2017).

5 See, for example, Martin Kragh and Sebastian Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: the Swedish Case," *Journal of Strategic Studies* 40, no. 6 (2017): 773-816, https://doi.org/10.1080/01402390.2016.1273830.

tries,[6] which focus on the so-called 'Gerasimov doctrine' of *maskirovka*, of operating below the threshold of open, conventional warfare while maintaining plausible deniability of involvement.[7] In contrast, this paper describes some of the tactics deployed in support of forces often (but not always) operating in a conventional manner, which are enhanced through the use of new technologies that afford greater penetration of asymmetric actions into critical elements and vital systems of the opponent. In other words, critical elements of a system are significant key elements (components, subsystems) of different systems (referring to fissures, weak points in a system).[8] Pressure on these weaknesses can lead to a cascading, synergetic, destructive systemic change (violations) of critical components and related systems.[9]

Application of hybrid warfare looks for more than critical vulnerabilities in hardware such as communications, infrastructure, or transport. Increasingly, state as well as non-state actors have attacked vulnerable points in ideologies and institutions, as well as taking advantage of social discontent or perceptions of corruption to level the conflict playing field.[10] These larger strategic fissures have allowed greater success for those undertaking information or asymmetric warfare against the West. The dominance of neoliberal ideas led to an increasing gap between rich and poor, and increased pressure of the middle class. As a result, there are fundamental changes in the economy, sociopolitical and psychological situation and reassessment of the core values, the growth of populism in many countries around the world. The Brexit vote in the UK in 2016 and the election of Donald Trump to the US presidency are reflective of this anxiety with socioeconomic conditions, calling into question decades-old institutions such as the European Union and NATO.[11]

---

6 Patrick J. Buchanan, *The Death of the West: How Dying Populations and Immigrant Invasions Imperil Our Country and Civilization* (New York: St. Martin's Griffin, 2002).

7 Andrew Monaghan, "The 'War' in Russia's 'Hybrid Warfare'," *Parameters* 45, no. 4 (2015): 65-74.

8 Brad Roberts, *Asymmetric Conflict 2010*, Report no. IDA-D-2538 (Alexandria, VA: Institute for Defense Analysis, 2000).

9 Vladimir Sazonov, Kristiina Müür and Holger Mölder, eds., *Russian Information Campaign Against the Ukrainian State and Defence Forces* (Tartu: NATO Strategic Communications Centre of Excellence and Estonian National Defence College, 2016), http://stratcomcoe.org/download/file/fid/7504.

10 Elīna Lange-Ionatamišvili, *Redefining Euro-Atlantic Values: Russia's Manipulative Techniques* (Riga: NATO Strategic Communications Centre of Excellence, 2016), http://stratcomcoe.org/download/file/fid/7350; Haroro J. Ingram, "Three traits of the Islamic State's information warfare," *The RUSI Journal* 159, no. 6 (2014): 4-11.

11 Ronald Inglehart and Pippa Norris, "Trump, Brexit, and the Rise of Populism: Economic Have-nots and Cultural Backlash," HKS Working Paper No. RWP16-026 (Harvard Kennedy School, 2016), https://www.hks.harvard.edu/publications/trump-brexit-and-rise-populism-economic-have-nots-and-cultural-backlash.

Preserving competitiveness and leading roles on the world stage requires appropriate economic power and a high level of education and science development, resources available mainly for centers of world power. Countries, lacking such access, may feel left behind, and the loss of opportunities and the rate of high-tech development in economic and defense sectors inevitably leads to the loss of their leading position and the redistribution of spheres of influence among more powerful actors. Striving to take control over competing "centers of world power" and to obtain unhindered access to strategic resources or, in contrary, to prevent such development of a situation, leads to violation or absorption of their security zones and spheres of influence. As a result, there is a dangerous mutual rapprochement of centers of world power with inevitable conflict of interests.

These conflicts are defined in Huntington-type civilizational clashes, with people's cultural and religious identities as the primary source of conflict in the post-Cold War world. American political scientist Samuel Huntington argued that future wars would be fought not between countries, but between cultures.[12] Clashes can also be Machiavellian attempts at undermining strategic adversaries, and leaders will often perceive a need to develop military power projection, that does not result in the *ultima ratio regum*[13] decisions, where violent conflict results in destruction for both sides. Instead, there is a necessity for new tools to achieve goals without direct and visible aggression.

The desire was for technologies that could provide not only new power of armaments, but also the ability to exploit weak points in all spheres of functioning of a state. In contrast to information campaigns of the past, new technologies allow the possibility to achieve strategic goals by unconventional and cognitive effects (technologies of social influence and manipulation, cyber sphere, information weapon, possibilities of significant damage of control systems of a state). Technologies, such as social media, made it possible for an actor to remotely influence all main institutions and infrastructure of a state. It formed a basis for unconventional invasions of territory, often even without the use of the conventional military components. Or its presence made possible externally organized and supported resistance movements and terrorism, which could also achieve strategic goals of uncertainty and institutional damage without violence.[14]

Thus, the "hybrid war" is a high-tech conflict. It is a continuation of the policy of a state and/or coalitions, political groups, transnational corporations, and non-state actors. The purpose of the conflict is to impose an actor's will on their opponents through integrated adaptive and asymmetric synchronized de-

[12] Samuel P. Huntington, "The Clash of Civilizations," *Foreign Affairs* 72, no. 3 (Summer 1993): 22-49.

[13] The final argument of kings (a resort to arms).

[14] Sergey G. Chekinov and Sergey A. Bogdanov, "The Nature and Content of a New-Generation War," *Military Thought* 4 (2013): 12-23 (in Russian).

structive effects on them in a multidimensional space and in various spheres of life. Hybrid war is rationally combined with conventional and unconventional components, an emphasis on multiple sources and modes of attack, synergy of results and a high level of uncertainty for opponents of what final strategic goals may be.

In hybrid conflicts the main goals are taking control over society, influencing the mindsets of people, and manipulating people, who are responsible for making important decisions in a state. The enemy aims to manipulate core values, motivational factors and cultural basis, and the strategic, communicational and critical infrastructure of a country. This is achieved by complex, balanced realization of effects with the use of soft and hard power. That's why critical elements of systems, in other words, objects for asymmetric actions in hybrid conflicts, are significant for a system key element (components, subsystems) of state, political, diplomatic, social, technical, sociotechnical, energetic, financial, cyber, socio-cyber, information and other systems. The influence on them in the limits of optimal measures and correlations of space parameters, time and resources for the influencing party leads to desirable, goal-directed, fast, cascading, synergistic and destructive for system changes (violations) in their relations, structures, processes and results of functioning.

Hybrid War in Ukraine

One of the distinctive features of the "hybrid war" in Ukraine is how much it has occupied all aspects of social life, how wide-ranging, multidimensional and employing multifactorial information focused on both psychological and cyber sources. A good example of such activities is provided by the innovative and highly technical samples of weaponry and military hardware applied during the 2014 Crimea annexation, as well as the combat actions in the east of Ukraine[15] since 2014:

- Electronic warfare systems and complexes and other types of electronic countermeasures;
- Modern information and communications systems;
- Innovative weapon control systems;
- Integrated reconnaissance-strike complexes;
- Innovative, including automated, software;
- Complexes for conducting information-psychological activities and actions in cyber space;
- Environmental control and space systems;
- Robotic systems (especially unmanned aircraft complexes) and countermeasures.

[15] See the Russian Military Technologies website, http://www.rusarmy.com, and the site of the "Russian Weaponry" Information Agency, http://www.arms-expo.ru.

The technology did not exist on its own, but was a part of a larger and strategically designed campaign to undermine confidence in central institutions. The initial goal was to establish a general loss of civic confidence in the government of Ukraine by launching an information warfare campaign aimed at discrediting government authorities, Ukrainian Armed Forces authorities, and encouraging an increase in crime and separatism activities. This information campaign fostered socio-political destabilization in the country and continues to negatively affect the country.[16]

This strategy successfully integrated innovative cyber technologies in coordination with carefully planned unconventional and irregular forces on the ground, leading to the 2014 annexation of Crimea and the military conflict in South-Eastern Ukraine. In response to both unconventional and conventional security threats, as mentioned above, most countries with rapid response capabilities focus on two primary components to their security apparatus:

- Deterrence potential, consisting of traditional branches of the armed forces (land forces, air forces, navy);
- Innovative warfare potential. The potential consists of military equipment and personnel of Special Operations forces, information-psychological operations and electronic warfare, as well as cyber forces (cyber intelligence, security and operations), branches of intelligence (electronic warfare, open-source intelligence (OSINT), technical types of intelligence, surveillance, and reconnaissance (ISR), etc.), operational control communication, military units, which are equipped with robotic (unmanned aircraft) complexes and countermeasures to associated attacks, other highly technological resources and measures.[17]

Generation of Highly Technological Warfare

Technological progress has always been a driving force behind military strategy. Technologically intensive wars are connected with design and wide use of advanced technical tools, and systems and complexes created by the most developed countries. These developments give certain countries a distinct advantage during combat actions without the necessity of massing overwhelming conventional forces. However, more technologically advanced states may be more vulnerable to certain attacks.[18]

---

[16] Jānis Bērziņš, "Russia's new generation warfare in Ukraine: Implications for Latvian Defense Policy," *Policy Paper* no. 02 (Riga: Center for Security and Strategic Research, National Defence Academy of Latvia, April 2014).

[17] Yuriy G. Danyk, D. Ishchenko, O. Manko, "Military Aspects of Advanced Technological Systems' Classification," *S.Korolov Zhytomyr Military Institute Scientific Journal* 8 (2013): 5-13 (in Ukrainian).

[18] Yuriy G. Danyk and O.O. Trush, "Specifics of Supporting National Security in an Environment of Advanced Technologies," *Government's Organization* 1 (2010), http://nbuv.gov.ua/UJRN/DeBu_2010_1_42 (in Ukrainian).

Photo 1: Application of innovative constructions of Jam-Proof Robotic Complexes by military personnel of S. Korolov Zhytomyr Military Institute.

New opportunities for targeting vulnerabilities, combined with new weapons and military equipment, led to the development, implementation and practical use in leading countries of new strategic concepts of warfighting: "Global Warfighting," "Global Visibility," "Global Coverage," "Net Centric Warfare," "Hybrid Wars," "Strategic Paralysis," "Parallel Wars," "Controlled Chaos" wars, "Unlimited Wars," "Controlled Wars," etc. These advanced concepts consider the combat effects on potential enemies from a distance via the use of intelligence information support, information and precision weaponry, robotic technologies, and other means. Innovative control technologies, as opposed to combat actions, allow attacks to be conducted primarily against priority targets with the maximum speed and precision of actions affecting "critical" components, over any territory of a state (region) without any physical presence required. The realization of such force projection allows the attainment of strategic objectives without the historic obstacles to victory of time, distance and intense manpower logistics. As long as the object of a security strategy is destabilization of one's opponent and exploitation of weaknesses in critical nodes (subsystems, components, objects), then it is not necessary to control territory by force. Rather, these vulnerabilities of security leakages, weak logistical links, security gaps, allow the disruption of essential systems necessary to continue or even initiate the fight. The dysfunction of the system or any other destructive impact on the target inhibits a state that has not been able to take preven-

tative measures to use its capability to respond adequately to subsequent warfare and warfighting.

In essence, state defense support, under conditions of hybrid threats and hybrid warfighting, demands the existence of a balanced and full-spectrum national security and defense sector. The armed forces remain the key component of national security, which must respond to modern and future challenges and threats. Armed forces should be equipped with supplies of advanced weapons and military equipment, relevant organization, and units staffed with skilled personnel. Skilled personnel should be able to conduct powerful information and special operations with the purpose of influencing economics, politics, energy systems, information and communications, command and control, local and enemy populations.

Military Components of Hybrid War

The peculiarities of the military component of highly technological and hybrid wars include:

- The transition from strategic control to operational combat control, the basis of which is real-time battlefield management and informational superiority over enemy actions: intelligence, decision-making and implementation, impacts (deprivation) [19]
- The transition of the primary warfighting responsibilities to cyber and airspace environments, including ISR [20]
- Warfighting means increasing based on robotization, stealth concepts, and warfighting from a distance
- The formation and use of situational and automated surveillance and attack complexes and systems
- Wide use of effective non-lethal weapons [21]
- The increasing use of irregular militia groups (paramilitary forces) [22]
- Related increase in asymmetric combat actions
- The increasing role and widening of Special Forces involvement [23]

---

[19] Joseph S. Nye, "Soft Power," *Foreign Policy* 80 (Autumn 1990): 153-171.

[20] David A. Deptula and James R. Marrs, "Global Distributed ISR Operations: The Changing Face of Warfare," *Joint Force Quarterly* 54 (2009): 110-115.

[21] Brian Rappert, *Non-lethal Weapons as Legitimizing Forces? Technology, Politics, and the Management of Conflict* (Abingdon, UK: Routledge, 2003).

[22] Frank G. Hoffman, "Complex Irregular Warfare: The Next Revolution in Military Affairs," *Orbis* 50, no. 3 (2006): 395-411.

[23] Dan Madden, Dick Hoffmann, Michael Johnson, Fred Krawchuk, John E. Peters, Linda Robinson, and Abby Doll, *Special warfare: The Missing Middle in US Coercive Options*. (Santa Monica, CA: RAND, 2014).

- The increasing reliance upon and use of radio-electronic, psychological and information warfare via cyber assets [24]
- The transition toward enemy-adapted warfare in all spheres of action.[25]

Information and Cyber Actions

A combination of research and combat analyses indicates that cyber-related actions and information warfare are increasing in both scope and importance for warfighters. In this context, hybrid warfare and the use of cyber assets as part of it is one of the most important factors for understanding the future arc of conflict. Combat actions in Illovaysk and Debalcevo in Ukraine were preceded by a significant burst of activity in information space. Negative information on key authorities of Armed Forces of Ukraine and government representatives was spread widely (usually outbursts of negative information in the Internet preceded the start of new combat campaign).[26] This is a common tactic, designated by Duggan as cyber aggression, coupled with disinformation from proxies and false fronts on the internet.[27]

Information and psychological operations (actions) of the enemy in cyber space require the use of different Internet resources. The examples of information and psychological operations are preparation and spreading of particular information in social nets and other Internet resources for discredit of Ukrainian authorities, ATO command and military personnel in the framework of campaigns "If not the Generals," "Generals-Betrayers of Ukraine," "Hail to the Ukrainian Artillery," etc. Disinformation or unchecked, false information including the use of special technologies of promoting the rates of such messages through Internet are often spread in national cyber space as military patriotic resources. It is necessary to mention that some Internet resources are hosted by the Russian Federation in Moscow [28] (Photo 2).

Content analysis and modeling of online news streams during the most intensive activities in Debalcevo in February 2015, utilizing the news monitoring technology "InfoStream,"[29] illustrate fluctuations of the amplitude to a degree critical to the spread of messages.

---

[24] Patrick M. Duggan, "Strategic Development of Special Warfare in Cyberspace," *Joint Force Quarterly* 79 (2015): 46-53.

[25] Vasyl M. Telelim, D.P. Muzychenko, and Yu.V. Punda, "Force Planning for the 'Hybrid War' Scenarios," *Science and Defense* 20, no. 3 (2014): 30-35. (in Ukrainian).

[26] For examples of the information operation to denigrate Ukraine's Armed Forces officials see "If only the Generals were not there," http://www.segodnia.ru/content/168270, https://topwar.ru/85589-esli-by-ne-generaly-pozornaya-istoriya-ukrainskoy-armii.html, http://colonelcassad.livejournal.com/2474409.html.

[27] Duggan, "Strategic Development of Special Warfare in Cyberspace."

[28] See, for example, http://wartime.org.ua.

[29] InfoStream – News Monitoring Technology, http://infostream.ua.

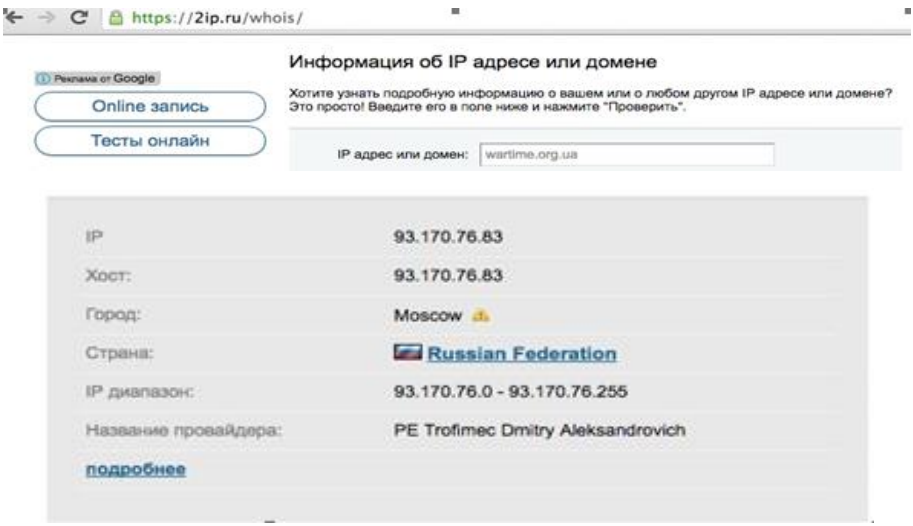

Photo 2. An example of Internet resource, discrediting Ukraine Armed Forces' authorities, hosted in the Russian Federation.[29]

Media analysis has demonstrated the significant consequences of mass usage of widespread, negative social political information campaigns. First, cyber aggression against key figures in government is expected to encourage the widening range of negative information streams in order to aggravate existing civil mistrust and anti-government behavior. When this is extended into social media, the spread of false and malicious information encourages beliefs and behavior that would normally be kept in check by existing social mores and civic expectations. Even if information does not create a conscious change in beliefs, it can impact the interpretation of future information by providing effective anchoring and priming media.[30] This can aid a domestic aggressor wishing to influence the course of the conflict in order to weaken support for the target government. In some cases, such information warfare can replace kinetic operations, undermining defensive campaigns before they even need to begin.

Cyber aggression often conceals its actors and motives, shrouded by technological methods that can mask their manipulative goals. The methods of concealment include anonymous claims to authority, news items manipulated with half-truths, repetition of messages, information overload, cyber-pseudo operations (government posing as insurgents), sock-puppeting (government agents playing the role of online commentators), and astro-turfing (creating of false grassroots movements).[31]

[30] Elizabeth Stoycheff and Erik C. Nisbet, "Priming the Costs of Conflict? Russian Public Opinion About the 2014 Crimean Conflict," *International Journal of Public Opinion Research* (2016): edw020. https://doi.org/10.1093/ijpor/edw020.

[31] Duggan, "Strategic Development of Special Warfare in Cyberspace."

In Ukraine, the consequences of such actions since 2014 have resulted in discrediting the Armed Forces, disaffection and mistrust directed toward the primary military and political authorities of the state, sowing of doubt concerning the necessity of military actions, and damage to civic morale and the encouragement of desertion among military personnel. In the absence of specific countermeasures against discrediting the Ukraine Armed Forces, disaffection and mistrust, one can expect as a result weakening of state and military capabilities needed to respond to aggression. Moreover, the actions of national media outlets, whether intentionally or not, organized by the Russian Federation, aggravated an already complex situation by appeals to encourage simple narratives. Media reliance upon untrustworthy or false sources, negatively-framed news stories, and criticism of the actions of Armed Forces' authorities contributed to the information campaign of the enemy.[32] Russian forces were able to exploit preexisting vulnerabilities in social, political, and economic systems leading up to open conflict, with the height of such operations coinciding with the onset of kinetic operations in Donbas in 2014. The use of cyber assets has been a form of force projection that helps initiate crises far ahead of and beyond the frontlines, creating forms of more complex crises that affect energy infrastructure, banking systems, and political leadership, and not solely the armed forces fighting on the frontlines. Again, the extension of traditional military conflict is not a new strategy, but new technologies have been able to provide both the means and vulnerabilities to allow such operations at a scale not often witnessed before, and with a smaller investment in resources on the part of the aggressor.

The effective prevention and detection of enemy's information and psychological actions in cyber space and our quick reaction require the creation of national centers of countermeasures to information and cyberattacks. The national centers should unite and facilitate coordination among international centers providing countermeasures to cyber threats. The national centers should provide monitoring and detection of destructive effects and identify signs, mechanisms (strategies, tactics, techniques, forms and methods) of their implementation. They should detect the sources and variants of spreading dangerous contents, interconnection during the operation (actions) among various Internet resources for defining the aim of the actions and possible results.

Measures for neutralization of destructive information and cyber effects and their sources are:

- Warning the owners (if they are known) of Internet resources about restrictions against spreading fake, untruthful information with the recommendation of its deletion if the information harms subjects and objects of national security (person, society, state)

[32] Sazonov, Müür and Mölder, eds., *Russian Information Campaign Against the Ukrainian State and Defence Forces.*

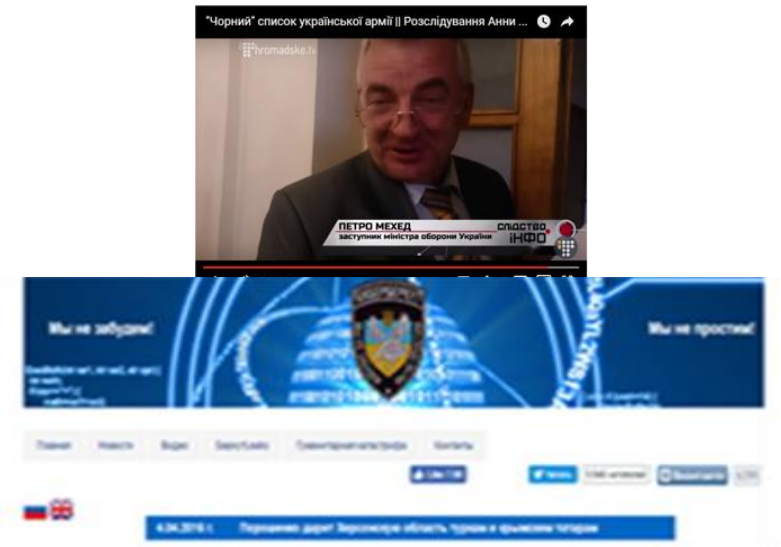

Photo 3. The example of reputation manipulation of Armed Forces authorities by mass media.[33]

- Creating public registries for unreliable/suspected resources.

In cases when it is impossible to define the owner or moderator, and the content may turn into a real threat to subjects and objects of national security, it is recommended to block electronic information resources, delete the content, etc.

Crisis Situations

Crisis situations appear as external forces (aggression and/or natural) exploit vulnerabilities and overwhelm critical systems in a target region or force. These crises can appear as a result of information and cyber actions in conditions of hybrid conflict, as a realization of information, psychological, and cyber threats

[33] "Cyber Berkut," https://cyber-berkut.org, is an Internet brand, which covers hacker attacks mainly at governmental and civil web-resources of Ukraine. The head of the brand is unknown. Jeffrey Carr, author of *Inside Cyber Warfare: Mapping the Cyber Underworld* (O'Reilly Media, 2009, 2011), considers it a group of Russian activists. The group describes its objectives, which include fight against neo-fascism, nationalism and the will of government in Ukraine. See also the TV Program on the First National TV channel of Ukraine "Black List of the Ukrainian Army" (part I), www.youtube.com/watch?v=BAlDnaG4VeM, and (part II), www.youtube.com/watch?v=ksydsCllv0g.

(e.g. terror, economic, military, diplomatic, politics, etc.) directed against critical infrastructures of a state or military force's command and control systems. This loss or intensive degradation of operability can be operationalized as a non-linear function, meaning that impacts may not be evident until the complete failure of the target system.

Effective countermeasures to crisis situations in cyber space according to ATO (the operation in occupied areas of Ukraine) experience can be realized in:

- Systematic development of forms, methods and means of operational detecting, protection and active countermeasures to information threats in cyber space
- Scientific research and development of specialized software and hardware capability for information activity in cyber space
- Professional military education and training based on combat experience and lessons learned in this sphere
- Conducting applied national and international training, war gaming and consultations
- Improving the training and education of military and civil specialists in the sphere of information and cyber security
- Operational implementation of lessons learned in national and international security systems.

Experience demonstrates that effective use of hybrid warfare methods results in largely unpredictable patterns of crisis and response. It is unusual for hybrid warfare practitioners to have clearly defined outcomes and event pathways, so likewise those responding to such strategies must be able to adapt in dynamic and rapidly shifting environments.

Technological design of well-known countermeasure systems in crisis situations, forms, methods and use of the systems must be oriented toward the formation of static excessive structure of a target system. The distribution of tasks among all components of cyberattacks on the system is often even, with a choice of components only according to their purpose. The increase of quantity and density of crisis situations' flow leads to structural complexity of systems designed to respond to them. This distributional design provides information redundancy of data and complication in its transfer and processing. The same principles are the basis for design of software aimed at realization of operational detecting processes, protection and active countermeasures to information threats in cyber space. The mentioned approaches are not efficient in real conditions of conflict where the enemy deploys equal or superior resources of information warfare, followed by soft power and kinetic forces to attain its objectives. This approach is a key feature of current hybrid wars.

Rigorous implementation of the principles of situational control provides opportunities for rational distribution and redistribution of own resources and focusing strengths on critical (for providing security) directions of enemy's ac-

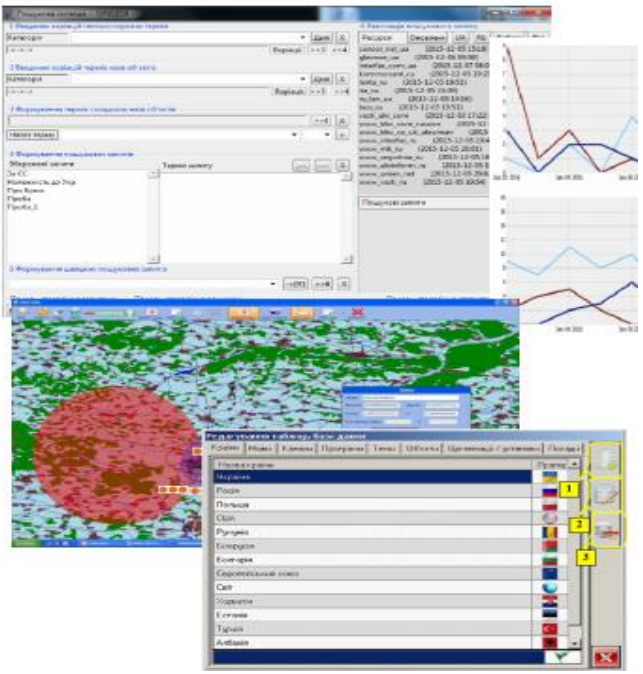

Photo 4. The formular view of one of the countermeasures complexes to psychological-information effects.

Photo.5 Automated system of information content-monitoring in social Internet services "Monitoring-C".

tions. Methods of fractal analysis, self-organization and bifurcation models give an opportunity to detect threats and critical situations in time, predict the direction of their development and real objectives.

Practically, this approach increases the effectiveness of information warfare countermeasures as a result of advance warning systems, the completeness and accuracy of information, and timeliness of reactions.

Hybrid War Spheres

A crucial consideration is the impact of the actions of an aggressor desiring to increase internal instability in multiple spheres (Fig. 2). Intended impacts can include increasing distrust in institutions and shared values, erosion of economic activity and trust, and a confusion of objectivity, expertise, ideology, and other sources of social cohesion.[34]

Hybrid wars differ significantly from traditional wars both in their initiation and prosecution, employing different strategies and means of operation. Hybrid warfare shares with irregular conflict (or IW – Irregular Warfare) the use of irregular or non-military forces, or at least those forces concealing their national allegiance in favor of anonymity or false camouflage as local militia. Special forces, sabotage-reconnaissance groups, intelligence units of various flavors are all involved in promoting and undertaking operations.[35] For some armed forces or state security forces, special operations can involve conducting specific information or cyber-related activities, electronic operations, or sabotage actions designed to destroy critical nodes that cannot otherwise be achieved via traditional means.

A high priority for state defense under contemporary conditions is therefore the design of effective countermeasure systems. Such systems should include technologically advanced types of intelligence, electronic intelligence, information and psychological operations, and cyber operations that can be coordinated to achieve a common strategy, as well as being able to operate both independently and as part of other operations.

A key component of such independent operability in both ISR and combat operations is the development and use of unmanned drones. The increasing use of drones for different functional areas (intelligence, electronic countermeasures, direct strikes, etc.) and different operational environments (land, sea, air, amphibious) is an important consideration for flexibility in dynamic conflict situations.

---

[34] Telelim, Muzychenko, and Punda, "Force Planning for the 'Hybrid War' Scenarios"; Kofman, "Russian Hybrid Warfare and Other Dark Arts"; Valeri Gerasimov, "The Value of Science in Prediction," *Military Industrious Courier Journal* 8 (2013): 1-3 (in Russian).

[35] Gerasimov, "The Value of Science in Prediction."

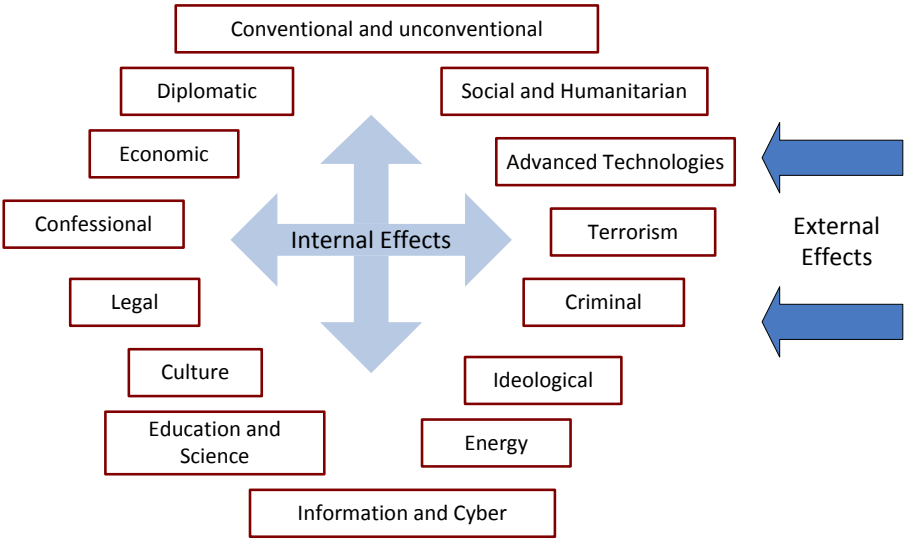

Figure 1: Hybrid War Spheres.

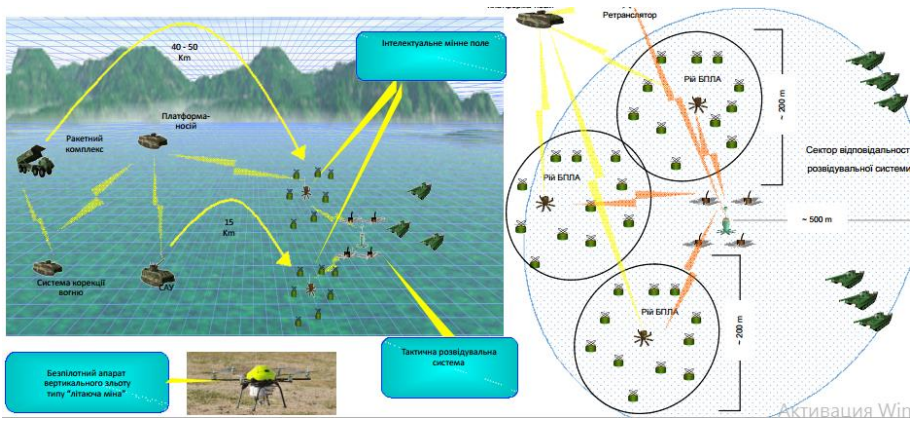

Photo 6. Unmanned Aircraft Complex of striking power for special operations like "Flying Mines."[36]

Deployment of advanced intelligence and response capabilities must be developed in parallel with appropriate training for both military and civilian personnel who will need to work within the system. Technology cannot be ex-

[36] This is a design of of the S.Korolov Zhytomyr Military Institute.

pected to work properly without highly skilled personnel who can use, maintain, and further develop the complex systems needed to address the shifting nature of the battlefield. Full, effective capabilities can only be expected when strategies and technologies are developed in coordination with professional training. The unprofessional use of such technologies is quite often the reason for their poor performance, as when standard operating procedures in training address much older conceptions of a problem (e.g. cyber intrusion into information networks as a technical issue, rather than a national security risk).

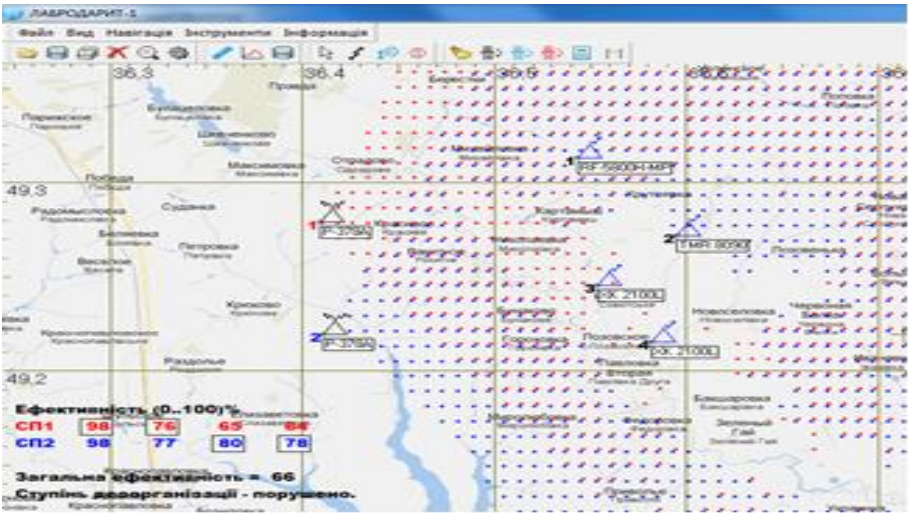

Photo 7. A screenshot from the electronic warfare planning system for planning the combat deployment of units.

The Advanced Defense Technologies Cluster

The state bears primary responsibility for the career management and training of defense personnel. Countries should therefore focus on the creation and development of technological defense systems, with integrated research and experimentation to provide appropriate levels of defense support. Extending the scope beyond the early warning available from 'hybrid threat' centers as established in some NATO countries, these clusters are intended to develop appropriate technologies and strategies for future threats they would be able to identify.

The envisioned Advanced Defense Technologies Cluster will include:

- A robust system of military research with proper scientific organizational structure
- Academic orientation toward expertise in advanced technologies

- Scientifically-based manufacturing complex, with stationary and mobile samples of weaponry and military equipment, command posts and laboratories
- Technologically advanced experimental combat and combat units, developed according to academic/scientific research of the cluster (Figure 2).

Practical military personnel training, testing and implementation of new technological systems of weaponry and military equipment, and the formation of new units must be based on developments by the defense technological cluster and active military units.

With respect to Ukraine, it is imperative to create a Military Scientific Technical Expert Center in advanced technological areas with the purpose of:

- avoiding double functioning of different organizations
- concentration in one place of efforts in research, design, creation, testing and use of advanced technological systems
- personnel training in areas of advanced technologies for all branches of the Armed Forces and for other ministries and establishments of the National Security and Defense Sector of the state

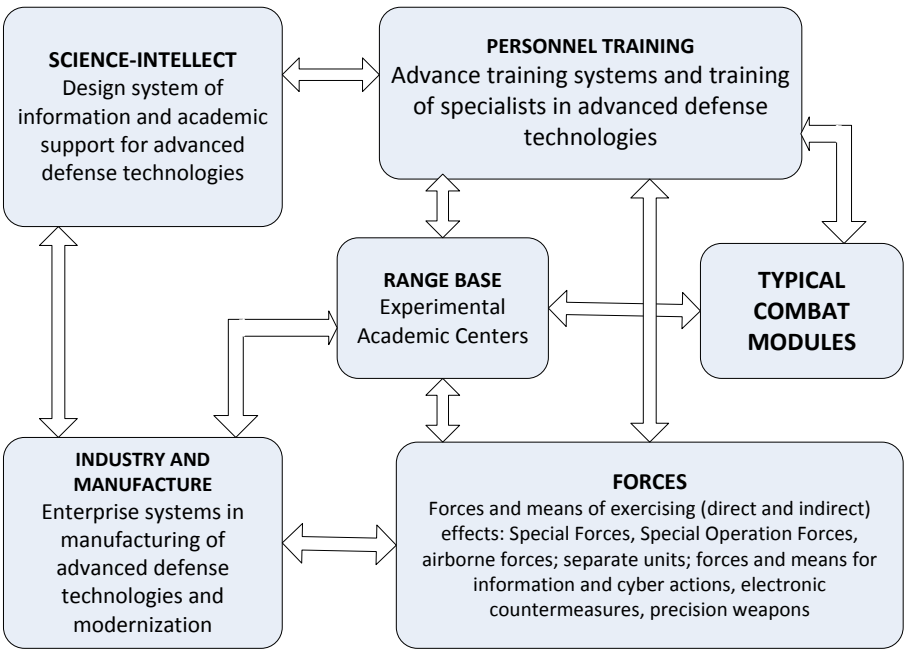

Figure 2: The Advanced Defense Technologies Cluster.

- use of the military component, industrial and manufacturing base of the region
- avoiding additional financial and temporary expenditures.

Practicability of the center can be substantiated and supported by relying upon experience of leading countries of the world gathered in the search of innovative ideas and their implementation in the military sphere, e.g. DARPA (the US Defense Advanced Research Projects Agency). Rational elaboration of all practical issues in the Advanced Defense Technologies Cluster must be conducted in close coordination with central military command and control organizations. It should work directly with forces cooperating with central control authorities. Central control authorities correspond with military units, and subdivisions with their range base and interacting organizations/ structures.

Conclusion

State policies of advanced technological, information and cyber security support systems have become among the most important components to consider with regards to national security policy in the military sphere. Modern technologies shift the ability to impact enemy forces, creating a need for reorganization to manage and defend against both soft and military effects, including in particular personnel training to maintain force readiness and continuity. The experiences of various countries that have already witnessed the new forms of hybrid warfare prove that national security and defense levels must be maintained even in conditions of world economic crisis and significantly decreased expenditures for the armed forces. The expansion of the battlefield beyond kinetic operations and infrastructure attacks demands complex use of both traditional force doctrines and new technological and synergistic planning.

The practice of military conflicts during the past decade demonstrates that the strategic advantage goes to the actor who first understands and implements new technologies, who can use them as a force multiplier and therefore overcome superior conventional forces – and often without even provoking a sustained response. Commanders must use the new methods, if only to understand the new methods and doctrines that the enemy can deploy. The use of advanced technological systems gives an opportunity to increase the effectiveness of already existing state military potential with lower expenditures, perhaps even by one third of traditional budgets. Considering the concepts of national security and national military strategies, governments of the most developed countries prioritize education and science for technologically intensive means of warfighting, implementing innovative control technologies, and providing for a fast and convincing victory in present and future military conflicts.

About the authors

Major General **Yuriy Danyk** is Professor and Doctor of Engineering Sciences. He graduated with honors from Zhytomyr Higher Military School of Radioelectronics, Kharkiv Military University (operational-tactical level), National Academy of Public Administration under the President of Ukraine, National University of Defense of Ukraine (operational-strategic level). He is an expert in the art of war, national defense and security, information and cyber security, electronic warfare, design and application of robotic complexes, and special forces development. He has combat experience in high technologies application.
E-mail: zhvinau@ukr.net

Tamara Maliarchuk holds a M.Sc. degree. Since 2013 she works for S.Korolov Zhytomyr Military Institute and in 2014 became a PhD candidate in Ivan Franko Zhytomyr State University. In 2014-2016 she attended e-Learning forums and workshops (in National Defense Academies in Romania and Bulgaria) organized by NATO countries and Partnership for Peace in e-learning application. In 2015 Tamara graduated the Military English Phraseology Course of the National Defense Academy, Warsaw, Poland. In May 2016 she studied at the Defense Language Institute, Lackland, San Antonio, Texas, USA. She conducts research in e-learning, innovative technologies in PTSD detection and therapy, manipulative technologies in web-environment. *E-mail*: maliarchuktamara@gmail.com

Dr. **Chad Briggs** is a Principal Consultant with Global INT. He has a PhD in political science from Carleton University in Canada, and specializes in translation of complex scientific data into risk assessments and strategic planning. He worked previously with the US Department of Energy on critical security assessments, and from 2010-2012 he was Minerva Chair of Energy and Environmental Security at the Air University, United States Air Force. He is a senior fellow at the Institute for Environmental Security in The Hague, professor of public policy at RIT Kosovo, and an adjunct professor of global security at Johns Hopkins University. *E-mail*: cbriggs9@jhu.edu.