Information & Security: An International Journal

Ivan Hristozov, v.39:3, 2018, 265-274 https://doi.org/10.11610/isij.3922

APPLICATION OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES AND MEANS OF RADIO-ELECTRONIC WARFARE IN HYBRID WAR

Ivan HRISTOZOV

Abstract: The development of science and technology leads to inventing new weapons and respectively new methods for conducting armed or unarmed conflicts. Based on practical examples, this article reveals the capabilities of some modern information and communications technologies and means of radio-electronic warfare that can be and are already used in hybrid war scenarios.

Keywords: hybrid threats; hybrid war, information and communication technologies, radio-electronic warfare.

Introduction

The armed struggle is only one of the forms of war. Confrontation between adversaries has always been characterized by implementing comprehensive strategies, based on combinations of conventional and unconventional resources, open and hidden actions of the military, paramilitary and civilian participants involving a wide spectrum of diplomatic, informational, military, economic, financial, intelligence, and legal (DIMEFIL) tools, all of which aim to achieve (geo-)political and strategic objectives. Currently, NATO and the European Union define such actions as hybrid threats.[2,**Error! Reference source not found.**] The hybrid model provides an opportunity to exert influence, pressure or destabilization of certain countries without leading to the use of military force and seizure of territory, although the use of open hostilities as part of a hybrid strategy may not be excluded.

The document "Vision: Bulgaria in NATO and in European defence 2020"[1] connects hybrid war with cyber war stating that the hybrid war "combines the application of conventional methods with techniques of guerrilla warfare, covert support to separatist groups, cyber attacks and propaganda, economic pressure and activities in breach of international law."

Seventeen types of military actions are described in US documents[7] – Acoustic Warfare; Antisubmarine Warfare; Biological Warfare; Chemical Warfare, Directed-Energy Warfare; Electronic Warfare; Guerrilla Warfare; Irregular Warfare; Mine Warfare; Multinational Warfare; Naval Coastal Warfare; Naval Expeditionary Warfare; Naval Special Warfare; Nuclear Warfare; Surface Warfare; Unconventional Warfare; and Under Sea Warfare. Thus, hybrid warfare may consist of a selection, and at times simultaneous forms of warfare across the spectrum of conflict, including all possible types or avoiding some of them.

Typically, opponents applying hybrid strategies seek to remain vague and unrecognized in their pursuit of legitimate goals; they try to keep their impact below a certain threshold, not causing a clear breach of international norms and preventing a coordinated response from the international community, i.e. avoiding where possible direct military confrontation.

New weapons and new respective methods of conducting armed struggle, new features and parameters of the war area have emerged with the development of science and technology. However, the basic principles of victory remain the same. Referring to the *operating environment*, the hybrid war has greatly expanded the field of clashes, as a "fifth field of battle" appears – military operations are conducted not just by land, sea, air, space but also in cyberspace. Some authors even mention another one, a sixth 'battlefield' – the human brain.

The development of information and communications technologies (ICT) is a prerequisite for their use as a weapon of hybrid war.

The purpose of this work is based on case studies to reveal the possibilities of some modern ICT (network technologies) and means of radio-electronic warfare (REW), used in hybrid wars.

New Information and Communications Technologies

Trends in the development of network technologies include:[6]

- Any device, to any content, in any manner;
- Online collaboration;
- Video communications;
- Cloud computing, etc.

The concept of any device, to *any content, in any manner*, is a major global trend that requires significant changes to the way devices are used. This trend is known as Bring Your Own Device (BYOD). BYOD is about end users having the freedom to use personal tools to access information and communicate across a business or campus network. With the growth of consumer devices, and the related drop in cost, people are expected to have some of the most advanced computing and networking tools for personal use. These personal tools include laptops, netbooks, tablets, smartphones, e-readers, etc.

BYOD refers to any device, owned by anyone, used anywhere. Extended connectivity, availability of new functions such as positioning and computational abilities (providing all necessary calculations in artillery shooting, for example,) make these devices applicable in warfare. Therefore, they may be tool for or subject of attack.

Online Collaboration

Not only do some individuals connect to a network to have an access to data applications, but they also need to collaborate with each other. Collaboration is defined as “the act of working with another [person] or others on a joint project.” [6] Collaboration tools, like Cisco WebEx, give employees, customers, military or non-military participants a way to instantly connect, interact, and achieve their objectives.

For businesses or military affairs, collaboration is a critical and strategic priority that organizations (military or paramilitary formations) are utilising to remain competitive. Collaboration is also a priority in hybrid activities.

Video Communications

Video is a useful tool for conducting business or military and other activities from a distance, both locally and globally. Today, businesses or military organisations are using video as a convenient way to do business, i.e. to conduct military or non-military operations.

Cloud Computing

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network. Companies use the hardware and software in the cloud, and they pay a service fee. In military, the term more often used is “network-enabled capabilities.”

Users do not need to have any software installed on their device. This allows many different kinds of devices to connect to the cloud. Users can access the information anyplace anytime by using a web browser.

Cloud computing is made possible by establishing, or using, data centres.

Solutions for Home Computing; Internet of Things

Networking trends do not only affect the way we communicate at work or at school, they also change almost every aspect of life at home.

The newest home trends include ‘smart home technology.’ Smart home technology is a technology that is integrated into everyday appliances, thus allowing them to interconnect with other devices, which makes them ‘smart’ or automated.

Application of New ICT Tools and Radio-electronic Combat in Hybrid Wars

Based on observation of the events in Ukraine, Syria and the Middle East, several basic methods can be distinguished for conducting a hybrid war with the use of new ICT: [8]

- Conducting information operations;
- Conducting psychological operations;
- Mass utilization of cyber attacks against important civilian infrastructure, military command and control, and logistics support;
- Behavioural war, i.e. targeted impact on the behaviour of large groups and structures in the opposing party that are potential source of danger;
- REW and use of directed energy weapons.

Information and Psychological Operations

From a theoretical and practical perspective, all military doctrines focus on the task of suppressing the will of the enemy, of subordinating and making it a tool for achieving goals. That is why one of the most important tasks in hybrid warfare is to manipulate the mass consciousness of society and influence the government – the president, ministers, members of Parliament and certain people responsible for making important decisions.

The manipulation of public awareness is critical for conducting hybrid operations. New ICT and contemporary social networks are an ideal environment for this. Israel has defined the hybrid warfare as a method of social warfare. In information operations, the weaknesses of institutions, discontent of local communities, minority groups and civil movements are used to create confusion in the contested population. It is possible for example, by conducting propaganda and psychological operations, to manipulate the ideology of a particular social group for different purposes such as radicalization or creating ethnic hatred. Tools for IT operations are also strategic communications. For this purpose, the media, including television, radio, newspapers and websites, can be bought. Social networks can be used to organize riots, as it happened in Ukraine or during the “Arab Spring” in Egypt, Libya, and Syria. Tension can escalate and lead to change of the political regime or even bring the country to a state of disaster. In his speech to students at the premier Academy for Martial Art in Moscow, General Gerasimov, Chief of General Staff of Russia, stated that the “colour revolutions" in North Africa, the Middle East, Georgia and Ukraine, NATO operations in Yugoslavia and Libya, demonstrate in practice that even 'successful' states may for months, or even days, become a scene of a brutal armed conflict as a result of foreign interference, and fall into a state of chaos, humanitarian catastrophe and civil war."[3,10]

Cyber Attacks

Network security is an integral part of computer networking, regardless of whether the network is limited to a home environment with a single connection to the Internet, or as large as a military or paramilitary organization with thousands of users (members).

Many external network security threats today are spread over the Internet. The most common external threats to networks include: [6]

- Viruses, worms, and Trojan horses – malicious software and arbitrary code running on a user device;
- Spyware and adware – software installed on a user device that secretly collects information about the user;
- Zero-day attacks, also called zero-hour attacks – an attack that occurs on the first day when a vulnerability becomes known;
- Hacker attacks – an attack by a knowledgeable person to user devices or network resources;
- Denial of service attacks – attacks designed to slow or crash applications and processes on a network device;
- Data interception and theft – an attack to capture private information from an organization's network;
- Identity theft – an attack to steal the log-in credentials of a user in order to access private data.

It is equally important to consider internal threats. There have been many studies that show that the most common data breaches happen because of internal users of a network. This can be attributed to lost or stolen devices, accidental misuse by employees and, in a business environment, even malevolent employees. With the creation of BYOD strategies, corporate data has become much more vulnerable. Therefore, while developing a security policy, it is important to address both external and internal security threats.

Richard Clarke, a US government security expert, has introduced the concept of "cyber warfare."[4] According to his definition, cyberwar refers to actions of a country to access computer networks of another country in order to cause damage and destruction. Recognizing the importance of cyberspace as early as 2009, the US government set up a Cyber Command (CYBERCOM), which is responsible for protecting the security of networks, leading computer intelligence, for prevention of cyber attacks and application of preventive strikes. With time, similar structures have appeared in the armies of other countries.

Apart from the above listed attacks, cyber space can be used for disinformation and propaganda,[18] participation of state-sponsored teams in political blogs, internet surveillance, persecution of cyber-dissidents and other activities. There are many examples of a number of denial-of-service attacks by competing organizations that have been organized as part of their cyber-warfare against each other,[17] most notably the 2007 cyberattacks on Estonia and the 2008 cyberattacks during the South Ossetian war of Russia against Georgia.

According to the cybersecurity firm CrowdStrike, from 2014 to 2016 the Russian hacker's team "Fancy Bear" used Android malware to target the Ukrainian Army's Rocket Forces and Artillery. They distributed an infected version of an Android application whose original purpose was to control targeting data for the D-30 Howitzer artillery. The application, used by Ukrainian officers, was loaded with the X-Agent spyware and posted online on military forums. CrowdStrike claims the attack was successful.

Another example is the cyber attack on the power grid of Ukraine: in December 2015, hackers managed to compromise the information systems of three electricity distribution companies.[14,19] Over 30 substations were excluded, and about 230,000 people remained without electricity for one to six hours. According to representatives of one the companies, the attacks were conducted from computers with IP addresses belonging to the Russian Federation.

The cyber attack was complex and consisted of the following steps: [2]

- prior compromise of corporate networks using spear-fishing emails with BlackEnergy malware;
- seizing supervisory control and data acquisition (SCADA) systems under control, remotely switching substations off;
- disabling/destroying IT infrastructure components (uninterruptible power supplies, modems, commutators);
- destruction of files stored on servers and workstations with the KillDisk malware;
- denial-of-service attack on a call-centre to deny consumers up-to-date information on the blackout.

The cyber attacks on energy distribution companies took place during an on-going Russian-Ukrainian war, and are attributed to a Russian advanced persistent threat group known as “Sandworm.”

Tolls for Radio-electronic Warfare and Directed Energy Weapons

Means for REW and directed energy weapons can be considered as weapons that benefit all opposing parties despite their different purposes. In most cases, military equipment is turned into a pile of metal, impossible to use. These weapons rarely cause casualties but they have a similar psychological impact on a potential adversary, and therefore, can be considered as a means of waging hybrid wars. There is a high variety of such tools.

In the fall of 2014, the Russian Su-24, which had on board the advanced REW complex “Khibiny,”[8] flew near the US ship Donald Cook in the Black Sea. It is claimed that the entire command and control system of the ship was out of order, including the missile complex “AEGIS.” All the crew panicked as the sailors had no idea how to manage the ship after the monitors went blank.

New weapons based on electromagnetic pulse[15] have led to a denial of all means of communication, complete discharge of the batteries in cars, tanks and other equipment, simultaneously with the discharge of batteries in mobile phones, in guidance systems and radio stations. Then the interruption of electrical circuits of all equipment has been developed. For example, a system for jamming,[16] exploding at a height of 200-300 meters may make defunct electronic equipment within a distance of 3.5 km: enemy units remain without communications, equipment for command and control, and the equipment should just be abandoned. The principle of this system’s operation is based on high-frequency generator of electromagnetic field with high power.

Other systems, such as “Rtut”[11] and “Ranets,”[15] lead to negation of certain types of guided weapons, like portable anti-aircraft missile complexes or antitank guided missiles, as well as fuses so that shells destroy themselves.

For protection of helicopters, the complex “President-C” has been developed.[13] Special sensors scan the airspace and when they detect a flying missile with infrared head, they submit a command to start the protection system. In the guiding system of the missile, a phantom image appears which misleads its electronic “brain” away from its primary target. The rocket rushes into the empty space and, after a certain period of time, destroys itself.

The system “Autobaza” allows to overtake the control system of unmanned aircrafts and disables their navigation systems and engines. Then they can be landed in a location of choice.

There are a number of devices for hidden protection against explosive devices and eavesdropping. For example, an instrument representing an emitter of noise,[16] is integrated into a small briefcase. This equipment conceals the lines of communication in all ranges, including GSM, and is capable of preventing activation of radio-controlled explosive devices within a few tens of meters. The apparatus can be used to provide security of movement of important people. It blocks the radio signals that can start detonation of an explosive device. The device "covers as a lid" certain space, thus blocking the actions of the receiving devices.

Conclusion

The analysis of the security environment confirms a trend of threats to national security which are becoming more dynamic, complex and difficult to predict. The Internet, new ICT and means for REW are both tools for and targets of hybrid attacks. In this regard, the focus on the essence of hybrid threats carried by them, the disclosure of their nature and defining the ways to counter them, has become a logical response to changes in today's security environment.

There is a need of capabilities to ensure information security, reliable cyber defence, effective protection of information in a common network environment, which provides the system of command and control. New tactics which make the opponent unable to respond effectively should be introduced. They should include the use of dominance in cyberspace, advancement of new information and communications technologies and modern means of REW.

Bibliography

1. *Vision 2020: Bulgaria in NATO and the European Defence* (Sofia: Ministry of Defence, September 2014).
2. VADM Rumen Nikolov, Chief of Defence, "Prospects for the Development of the Bulgarian Armed Forces in the Face of Hybrid Threats," Lecture at the "G.S. Rakovski" National Defence College, Sofia, September 2015, in Bulgarian, https://www.mod.bg/bg/doc/ministry/nachalnikOtbrana/20150901_Lekcia_VA.pdf, accessed December 1, 2015.
3. Petko Dimov, "Main Characteristics of the Operations' Environment and Algorithm of Hybrid War," *Military Journal* 123, no. 1 (2016): 86-96, in Bulgarian.
4. Richard Clark and Robert Nake, *World War III: What Will It Be Like? High Technologies in the Service of Militarism* (Piter, 2011) in Russian.
5. Adam Meyers, "Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units," *CrowdStrike*, 22 December 2016, https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/, accessed April 15, 2018.

6. “Cisco CCNA Introduction to Networks course,” *Cisco Networking Academy*, last modified September 2016, https://www.netacad.com/courses/ccna/, accessed October 12, 2016.
7. Davi M. D’Agostino, “Hybrid Warfare: Briefing to the Subcommittee on Terrorism, Unconventional Threats and Capabilities,” Committee on Armed Services, House of Representatives, 7 October 2014, https://geopolicraticus.wordpress.com/2014/10/07/hybrid-warfare, accessed October 30, 2016.
8. “EW Aircraft: Survive for a ‘Thick Veil’ of Interference,” *Army News*, November 21, 2014, in Russian, http://army-news.ru/2014/11/samolyoty-reb-vyzhit-za-gustoj-pelenoj-pomex/, accessed August 15, 2016.
9. “Complex EW ‘Krasukha – 4’,” *Military Review, News VPK*, December 19, 2013, in Russian, http://vpk.name/news/102419_kompleks_reb_krasuha4.html, accessed August 20, 2017.
10. Andrey Sushentsov, “Russian ‘Hybrid War’: Nothing New,” *Foreign Policy*, May 7, 2015, in Russian, http://www.foreignpolicy.ru/analyses/rossiyskaya-gibridnaya-voyna-nichego-novogo/, accessed May 2015.
11. “‘Mercury’ in the Russian army forces,” *Krasfun.ru*, July 31, 2014, accessed August 2016, in Russian, http://www.krasfun.ru/2014/07/rtut-v-vojskax-rf/, accessed October 30, 2016.
12. “Hybrid war – does it even exist?” *NATO Review Magazine*, 2015, accessed September 20, 2016, http://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN.
13. “The ‘President-C’ Averted a Missile Away from a Russian Mi-8 in Syria,” *EurAsia Daily*, October 12, 2016, in Russian, https://eadaily.com/ru/news/2016/10/12/prezident-s-otvyol-raketu-ot-rossiyskogo-mi-8-v-sirii?utm_source=smi2, accessed October 30, 2016.
14. “December 2015 Ukraine Power Grid Cyberattack,” *Wikipedia*, 23 December 2015, https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyber_attack, accessed May 23, 2016.
15. Timur Alimov, “‘Alabuga’ Will Make Useless Enemy Equipment,” *Russian weapons*, October 2, 2014, in Russian, https://rg.ru/2014/10/02/alabuga-site.html, accessed August 30, 2017.
16. Timur Alimov, “Russia Has Created a ‘Suitcase’ for Explosion Protection and Listening,” *Russian weapons*, May 6, 2016, in Russian, https://rg.ru/2016/05/06/v-rossii-sozdali-chemodanchik-dlia-zashchity.html, accessed August 23, 2017.
17. Kenneth Geers, “Cyberspace and the Changing Nature of Warfare,” *SC Magazine U.S.*, August 2008, https://www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/554872/, accessed May 23, 2016.
18. Pete Earley, *Comrade J: The Untold Secrets of Russia’s Master Spy in America After the End of the Cold War* (New York: Penguin Books, 2009), 194-195.

19. Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case," Protocol TLP: White, E-ISAC, SANS-ICS, 18 March 2016, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, accessed May 12, 2018.

About the author

Col. Ivan Hristozov is Associate professor and deputy director of the *Defence Advanced Research Institute* at the "G.S. Rakovski" National Defence College. His primary research interests are experience is in development and implementation of communications and information technologies and systems for the purposes of national security and defence**.**