CONSIDERATIONS REGARDING INFORMATION WARFARE AND COMPETITIONS IN THE CURRENT GLOBAL SECURITY ENVIRONMENT

Constantin RAICU

Independent researcher / Brasov / Romania

Abstract:
The idea of warfare using information as a weapon is not new. Yet, many experts from different countries consider information warfare more and more actual, due to the evolution of information technology. The recent attention given to information warfare does not mark the birth of a new form of conflict. Rather, it marks a significant change in the implications of an old one.

This is the main idea that embraces the approach of the present paper. By comparing different views on information warfare, through the evolution of global security environment, we are better able to understand from the opposite perspectives which are the security issues that challenge the actors or might become opportunities for them to prevail. Also, hybrid warfare is equally one of the major challenges that nations face in current times and therefore it must be considered increasingly more.

Moreover, information warfare implications in the current global security environment can be better understood to the extent that it is observed and analyzed in the context of recent conflicts.

Key words: information warfare, information operations, information environment, (critical) information infrastructure, information technology, hybrid warfare, cyber warfare, global stakeholders.

1.Introduction

Many people today are talking about the impact of information technology on the world. They are discussing how the economy, business, education, and even personal relationships are being affected by the onset of the information age. It should come as no surprise, then, that people are also talking about how technology is impacting the way we engage in one of our oldest traditions - war. The term "information warfare" has been in use for a number of years now, intended to represent whatever warfare is becoming in the information-centric 21st century. Unfortunately, though, many people use this term without really knowing what it means. In an effort to make progress toward a common definition, this paper presents one possibility and expands on it by discussing the weapons, strategies, and countermeasures involved in "information warfare", as defined.

Since the early 19th century, the well-known Prussian political thinker and soldier, Carl von Clausewitz, stated in his famous work *"On War"* that *"War is merely the continuation of policy by other means"*, where the original German term *Politik* means both politics and policy combined. Clausewitz clearly recognized that war is just a tool, but not the objective itself, when he stated that *"War is thus an act of force to compel our enemy to do our will"*[1].

[1] Clausewitz, C., *On War*, Project Gutenberg, http://www.gutenberg.org/ files/1946/1946-h/1946-h.htm

Today, the information warfare (IW) is such political tool but is not applied in the violent manner of a classic war. And, because IW is conducted silently, it remains almost invisible for the public perception. Due to that low level of awareness, the political strategists have understood that is easier and more effective to act behind the curtain in order to achieve national goals. Such arena today is “cyberspace” but the ground of hostilities is far more extended.

Firstly, not all of information warfare types are necessarily related to sophisticated technology and cyberspace. Information warfare could embrace many other methods, more related to the human factor. For instance, unlike western approaches - which are more focused on cyber warfare, eastern powers like Russian Federation and even China still continue to develop certain types of unconventional warfare, many of them being relied on the use of psychological influence, deception, media operations or legal warfare.

Secondly, it is a fact that, in this information age, the spectrum of competition for resources has already exceeded the military dimension and almost erased the difference between peace and war. Today, many governments invest significant efforts in adapting and upgrading some information-based means of confrontation that were similar to those used in the period during the Cold War, in order to secure or expand their power and influence around the world.

Thirdly, through information warfare, the boundary between military and non-military domains has become blurred. Many non-state actors are interested in developing information-based capabilities, both defensive and offensive. Corporations, especially, consider IW tools very useful when competing with each other for a dominant position on the market.

Consequently, the increasing complexity of the overall arena around cyber warfare challenges both nations and international organizations in managing the information environment, according to their security interests. Today, in cyberspace and not only, the critical information infrastructure has become a permanent target to information attacks, a major concern and a top priority for key-decision makers to constantly implement updated strategies and more suitable protective policies.

2. Information Warfare Conceptual Framework

2.1 General considerations on IW. Back to the emergence of the concept

One of the problems with information warfare (IW) was that for a long time no official definition existed. The main reason for this is that this kind of warfare is relatively new and that the term IW has many different meanings. On the one hand, there is the military aspect of it but on the other hand, IW is also used to describe the “war on the Internet”.

Actually, the term information warfare appeared first in the US military doctrine about 25 years ago, at the end of the Cold War, as a concept that encompasses in an integrated manner a multiple use of information systems and communication technology for both offensive and defensive purposes. The vision behind this concept was to design, develop and employ suitable information capabilities that could affect the adversary political, military, social and economic pillars which sustain his power during peace and war.

Yet, from the beginning, the IW has not been only a military-related concept. As the entire world was connected and influenced by the development of information and communications technology, numerous researchers have become aware and understood the new risks and vulnerabilities from the cyberspace, especially in the areas of the economy (banking, business, marketing, generally information-based activities) (see fig. 1). It could go further, as online espionage, generating national security breaches to get sensitive or classified information through the use of Internet or, eventually, as sabotaging acts in order to disrupt critical communications networks or to disable the control of key industrial facilities (nuclear plants, power generation and transmission systems, oil and gas pipelines, water collection, treatment and distribution infrastructure, etc.).

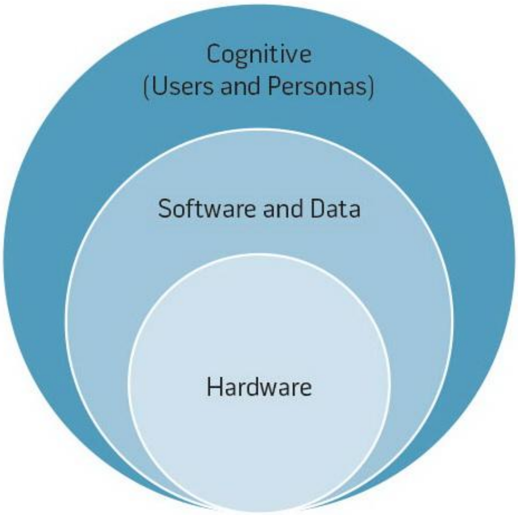

Fig. 1 Cyberspace components

Referring to that, three years before to write his book *"Information warfare: Chaos on the Electronic Superhighway"*, Winn Schwartau[2] put in 1991 these cyber threats into three classes, with specific consequences at each level of society:

- *Personal*, where individuals suffer identity theft and privacy is severely affected;
- *Corporate*, where private companies conduct unethical attacks on each other in order to prevail on the market;
- *Global*, where countries, NGOs, terrorist organizations, use information warfare sophisticated weapons to fulfill their hidden agenda.

According to this, a multitude of social activities was expected to be targeted in the new information environment (IE): media transmission jammed or hijacked, logistic or communications networks disabled, business transactions sabotaged, power grids interrupted, databases corrupted or even confidential information stolen.

But the Internet is only a small part of the areas in which IW can produce significant damage. Although the Internet touches many from critical infrastructures and, as an interface, influence their information environment, other areas of IW remain outside of it. Any forms of social education and media can be used as a vehicle for IW – magazines, newspapers, radio, television, cinemas, schools, professional unions, public conferences, seminars, advertising leaflets, e-mailing, web pages or social media. Clearly, IW is extended much more than attacking computers with malicious codes.

IW is struggling to link together all the areas that form the IE, crossing national borders, social conditions, and cultural views. It is a synchronized and coherent manner that could embrace all the resources of a government, corporation or international agency

[2] Schwartau, W., American expert on security, privacy, info war, cyber-terrorism and related topics, author of
Information Warfare: Chaos on the Electronic Superhighway, 1994

to control the IE in order to gain and maintain a competitive advantage, power, and influence.

When properly conducted, IW is a flexible full spectrum of capabilities that can be adapted to any situation. It can be applied in both the virtual and physical worlds. The consequences could be dramatic. Attacks can be devastating, such as social disruptions or breakdowns of critical infrastructure capabilities (power grids, transportation, communication, and finance). An offensive IW is able to make a government, a corporation or a bank bend to the will of the attacker. The chain of IW effects could prevent a country to project effectively its political, military, economic and administrative power. The key purpose is to influence the decision makers or those who manage resources and resources-based information.

2.2 The Military Outlook on the IW. Some attempts to define it

Regarding IW, however, from a military perspective, I cannot totally agree upon its asymmetric features. I am still confident that such unconventional assets could fall into the hand of certain hostile non-state actors at some point and apply their effects against military parties. But that is not always so. The major issue here, which makes the difference from asymmetric warfare, is that, for instance, the corporations themselves or any business organizations fight each other in the same spectrum of IW.

Consequently, because of its multiple faces, it is hard to encompass IW in a complete definition. This difficulty, also, was remarked by Martin C. Libicki[3] in an article written in 1995, saying that *"there is little that is not information warfare."*

Applying IW has multiple advantages in comparison with the symmetric means of a classic war. It can be executed without using physical destruction; it is cheaper to be deployed than ordinary weapons and does not require large number of troops; it can achieve instant effects and remove the inherent delay when employing conventional assets; the physical proximity to a target is not necessary and also, provides the ability to conduct anonymous attacks.

There are a lot of interpretations, broad or narrow, within the national and international business, governments and academic research communities, of what information warfare means. Some of them even reject the notion of it. Different governments, agencies, and organizations have a wide range of approaches and policies, mainly depending on their strategic interests, technological capabilities and circumstances imposed by environmental interconnections.

Even today, its ambiguity raises difficulties for theorists. Through IW, there is a blurred boundary between conflict and peace, advantages and vulnerabilities, competition and cooperation, as well as between military and non-military ways to wage wars.

Although IW was embracing, at that time, specific human-related aspects of information use, closely linked to psychological warfare, US military tended to focus on technology instead, extending the IW concept into the realms of electronic warfare (EW), cyber warfare, command and control warfare (CCW) and computer network operations (CNO) (see fig. 2).

[3] Libicki, M. C., American IW theorist, author of *Who Runs What in the Global Information Grid (2000), Conquest in Cyberspace: National Security and Information Warfare (2007), Cyberdeterrence and Cyberwar (2009)*

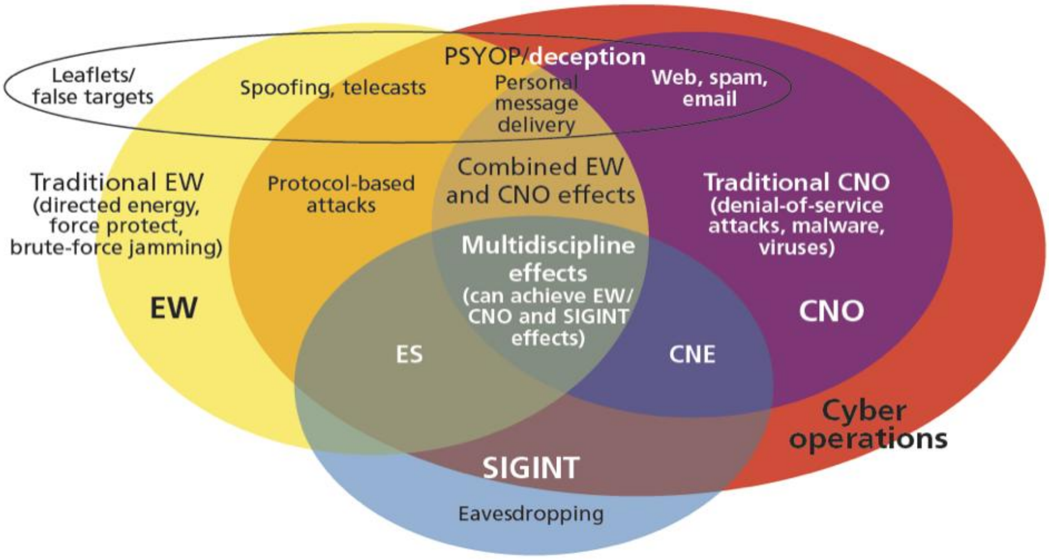
Leaflets/ false targets
Spoofing, telecasts
PSYOP/deception
Personal message delivery
Web, spam, email
Traditional EW (directed energy, force protect, brute-force jamming)
Protocol-based attacks
Combined EW and CNO effects
Traditional CNO (denial-of-service attacks, malware, viruses)
Multidiscipline effects (can achieve EW/ CNO and SIGINT effects)
EW
ES
CNE
CNO
Cyber operations
SIGINT
Eavesdropping

Fig. 2 Functional view of IW converging areas[4]

It is interesting to observe here that there is a close bond between the Cold War as a competition for global dominance and the emergence of IW concept at the end of this period with its multiple effects at all levels of a confrontation. Beyond the consideration that IW may be an inheritance of the Cold War, I actually believe that, through this concept, this race between west and east superpowers is still ongoing.

Nonetheless, a recent comprehensive study published by the Washington-based Center for Strategic and International Studies (CSIS) classifies information warfare activities according to the source, the form, and the tactical objectives of the attack. Therefore, the information war can be seen as a conjunction of the three dimensions.

Firstly, an attack could arise either from outside or from within the targeted organization or system. Secondly, four categories of attack can be identified:

- *Data attacks*, conducted by inserting data into a system to make it malfunction;
- *Software attacks* (similar to data attacks), conducted by penetrating systems with software causing failure or making them perform other functions than those intended;
- *Cracking or hacking*, seizing or attempting to seize control of an information system (or a vital part of it) to deny use, disrupt, steal data or resources, or cause any other kind of harm.
- *Physical attacks*, the traditional form of attack (assaulting, bombing, and destroying) straightened against information systems. An electromagnetic pulse (EMP) produced by nuclear explosions can also be included in this kind of attack.

All these different forms of information warfare attack can be classified by their goals or tactical objectives: they could be focused on deception, exploitation, disruption or destruction of information systems [5] (see fig. 3).

[4] Porsche, I. R. et al., *Redefining Information Warfare Boundaries for an Army in a Wireless World*, RAND Corporation, 2013, p.51

[5] *Cyber-crime, Cyberterrorism, Cyberwarfare Averting an Electronic Waterloo,* CSIS Task Force Report, Center for Strategic and International Studies, Washington DC, 1998, pp.9-11

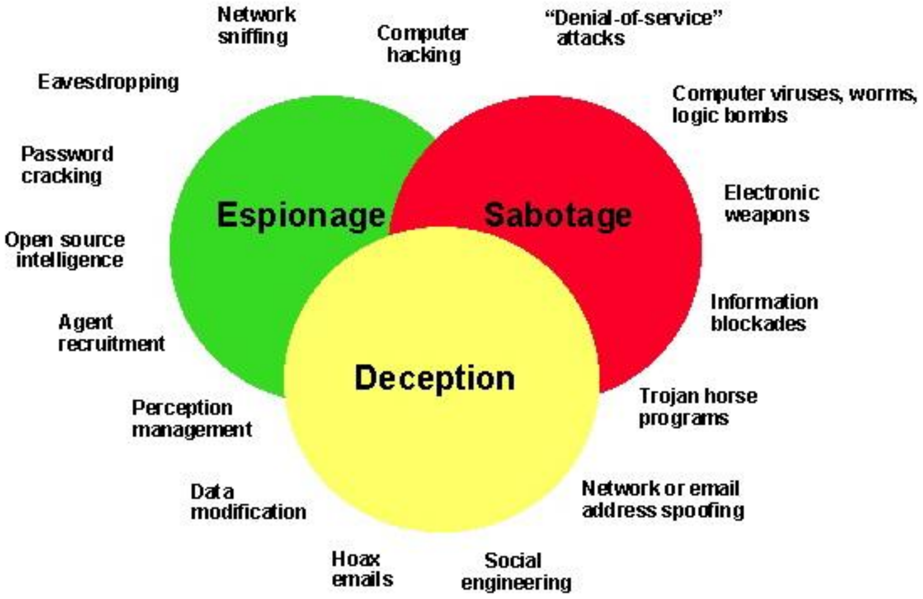

Fig. 3 The world of information warfare

Although there are many accurate and acceptable definitions, I can try to summarize them into a simpler and more limited formula. Information warfare could be then defined as *"defensive and offensive operations, conducted by individuals or structured organizations with specific strategic and political goals, for the exploitation, disruption or destruction of data available in computers or transmitted over the Internet and other networked information systems".*[6]

Early, in 1996, the US Department of the Army released FM 100-6, a field manual for information operations (IOs), in which IOs takes place in a global environment, being defined as *"continuous military operations within the military information environment that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations. IOs include interacting with the global information environment and exploiting or denying an adversary's information and decision capabilities."*

When, later, in 2006, the IW term was definitely eliminated[7] from the US doctrine, the preferred concept of *Information Operations* (IO) produced instead much confusion, being assimilated with that of psychological operations (PSYOPS). Even more, as the Joint Publication 3-13, Joint Doctrine for Information Operations, was revised and republished in 2012, IO was still not separated from exclusive war purposes. According to the definition, IO were seen as "*the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.*"

[6] Lorenzo, V., *Information requirements for Information Warfare: the need for a multidisciplinary approach*, presentation prepared for the 1999 Info War Conference, 27 May 1999, London; and George Ballantyne, "www.terrorism.now", RUSI News brief, April 1999, p.31. From letter by John J. Hamre published in Issues in Science and Technology, Winter 1998-99, pp.10-11

[7] it was revised the US Joint Publication 3-13, Joint Doctrine for Information Operations

However, the interchangeable view between IW or IO concepts was not entirely useful in my opinion. Clearly, to maintain such concept in the US military approach merely meant, at that time, allowing to the Eastern opponent (Russia) to recognize indirectly the intended extension of the old confrontation.

3. IW Between Opposite Perspectives - East vs. West

3.1 The Russian Federation. The Devil Is In Details

The Russian view, which is still anchored in the period during the Soviet Union, considers the information through its vehicle as taking an artificial or natural form. Unlike in the western approaches, the cyber domain is not one of priority concern, being seen as just one component among others, including social, human and spiritual domains. As a result, it is not perceived separated but related to all other suitable means to conduct information operations.

Therefore, information warfare takes on different meanings in the Russian Federation. While the Western countries focus on “information operations” as distinct from concrete acts of war, Russian doctrine specifically talks about war. According to this doctrine information warfare is defined as follows: *“Confrontation between two or more states in the information space to damage the information systems, resources, and processes, which are of critical importance, and other structures, to undermine the political, social and economic system, and effect massive brainwashing of the population for destabilizing the state and the society, and also forcing the state to make decisions in the interests of the confronting party.”*[8]

Therefore, the Russian theory has been built in opposition to cyber security theory developed in the United States and Western Europe primarily concerning the use of new computer technologies for military and intelligence purposes, namely the activity in cyberspace. This involved transferring Western terminology across to the Russian world. However, a strong emphasis was put on the “defensive” nature of the Russian theory, when it was being adapted to Russian reality.

Russian terminology is intentionally confusing for becoming such a manipulative trick, which has been confirmed by a critical review of the key terms. Thereby, they cannot be made to fit in with any of the definitions used in the West. On this line, the terms as “information warfare”, “cybernetic warfare”, and “network warfare” have completely different meanings in Russian view. Most Russian theoreticians understand “information warfare” as influencing the awareness of the masses as part of the rivalry between the different civilizational systems adopted by different countries in the information space by use of special means to control information resources as “information weapons”.

They thus mix the military and non-military order and the technological (cyberspace) and social order (information space) by definition and make direct references to “Cold War” and “psychological warfare” between the West and the East.

As a result, the term is usually placed in two contexts:

- *The geopolitical rivalry between Russia and the West* (above all, the USA and NATO), and it has a political, an ideological and a cultural dimension;

[8] *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space,* 2011, https://ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf

- *The tasks set as part of the Information Security Doctrine of the Russian Federation*[9].

According to specialists from the secret services and the Russian Security Council, this strategy excessively narrowed down the information security subject. Cyberspace security is treated as a broken term, although it is emphasized that new technologies have expanded the arsenal of means used to influence public opinion. It is interesting to note that the technological aspect (cyber) is underrepresented in the public space and it is evidently kept confidential.

Including support of the regime in the core interests of the state ensures that civil society is an integral part of national security operations. Current Russian doctrine, and therefore leadership operates under the idea that regime security and national security are the same.

In 1995, four years after the emergence of World Wide Web, the IW theorist Vitaliy Tsygichko observed that "*the development of an international information superhighway would create new conditions for the effective employment of information weapons*"[10].

Since 1998, Russia has pleaded multiple times within the Security Council of United Nations (UN), to obtain an international agreement on countering the information terrorism. The main concern was that the mere use of the Internet by a foreign government could challenge very easy the political stability in other countries.

Moreover, the psychological warfare is named as a key threat to Russian national security and sovereignty. Russia's first Information Security Doctrine document was published in 2000.

Since 2001, Russia has adopted a triple approach in order to consolidate its stability in the newly information environment: international, internal and military. On the international front, it has continued the efforts to influence the opinions at the UN and through SCO (Shanghai Cooperation Organization) or other international conferences. Internally, there were implemented specific doctrines and policies to increase the information security against cyber-crimes, and to improve the social-psychological balance with the regard to the impact of news media on the Russian population. In the military domain, Russian Federation was involved in the modernization of its military strategy and capabilities in order to meet the requirements imposed by the international environment changes.

In 2009, on a meeting of the Shanghai Cooperation Organization (SCO)[11], the members proposed cooperation at the state level with regard to the threats related to international information security. The members agreed on three main concerns to decrease: the preparation and conduct of information warfare, information terrorism, and information crime.

One year later, in 2010, within the Military Doctrine[12] of Russian Federation, is mentioned *"the intensification of the role of information warfare"* with the requirement *"to develop forces and resources for information warfare"*. However, this was a late and, somehow, duplicitous official statement, because in 2007 in Estonia and then in 2008

[9] Darczewska, J., *The Anatomy of Russian Information Warfare*, Centre for Eastern Studies, Warsaw, 2014, p.12

[10] https://ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf

[11] SCO was founded in 2001 by China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan. The stated main goal was to strengthen mutual confidence and good-neighborly relations among the member countries

[12] see http://www.sras.org/military_doctrine_russian_federation_2010

during the war with Georgia, there was evidence regarding the use of cyber-attacks by Russian Federation. Thereby, in April 2007, multiple cyber-attacks were mounted against Estonia during a disagreement with Russia about the relocation of the Bronze Soldier of Tallinn memorial. A number of Estonian organizations were attacked, including the parliament, ministries, banks and media. During the invasion of Georgia, there was a clear demonstration of a combined cyber and kinetic attacks by Russia. Although not completely successful, it might reflect the Russian approach.

Also, in 2013, Russian Federation released the Russian foreign policy in which is stated that there will be taken *"necessary measures to ensure national and international information security, prevent political, economic and social threats to the state's security that emerge in information space in order to combat terrorism and other criminal threats"*. According to this, from a Russian military perspective, the use of information warfare against Russia will not be considered a non-military phase of a conflict whether is conducted or not against its military forces.

Increasingly more, Russia is considered one of the greatest powers in terms of offensive cyber capabilities. According to the 2015 "Worldwide Threat Assessment of the US Intelligence Community", the Kremlin was establishing a Cyber Command similar to the Americans' CYBERCOM – a center for directing offensive propaganda operations and cyber-attacks. Furthermore, this report notes the ability of Russian "cyber actors" to penetrate industrial control centers. Using malware, these actors will be able to affect the systems of critical enemy infrastructures.

The Crimean operation was an opportunity for Russia to show to the entire world the potential and the capabilities of information warfare. Its purpose was to identify methods to subordinate the societies and the elites in other countries by using various kinds of open and secret channels (secret services, diplomacy, and media), psychological impact, and political and ideological sabotage.

Russian information warfare is set to continue since Putin's new doctrine has formed. This doctrine is Eurasian, geopolitical, anti-liberal and oriented towards rivalry with the West and Russia's dominance in Eurasia. For this reason, the key tasks of the rational public debate are and will continue in the immediate future to be to set limits on the space available to Russian political myths and ideologized propaganda actions, and to explain the mechanisms and goals of such actions.[13]

Cyber aggression has jurisdictional and legal aspects. There are a gap and a fundamental divergence between the Russian and USA views on the need to regulate hostile activities on the Internet. The US standpoint is that a treaty is unnecessary. Instead, the USA advocates improved cooperation among international law enforcement groups. By cooperating to make cyberspace more secure against criminal intrusion, their work will also lead to improved security for military campaigns.[14] The USA are also resistant to any agreement that would allow governments to censor the Internet in favor of totalitarian regimes.

The Russian view is the opposite. From a Russian perspective, the absence of a treaty is permitting a kind of arms race that could have unpredicted consequences. The IW weapon' should be taken into account in disarmament negotiations in a way similar to the generalized potentials of groupings of troops (forces, weapons, combat equipment, etc.). Russia has proposed a disarmament treaty that would ban a country from secretly

[13] Hunter, E., *The Challenges of Hybrid Warfare,* International Centre for Defence Security, Estonia, 2015, p.6

[14] Markoff, J., Kramer, A. (2009) *U.S. and Russia Differ on Treaty for Cyberspace*, New York Times, 27 June 2009: http://www.nytimes.com/2009/06/28/world/28cyber.html?_r=2&partner=rss&emc=rss

embedding malicious codes or circuitry that could later be activated remotely in the event of war.[15] Other Russian proposals include the application of humanitarian laws banning attacks on non-combatants and a ban on deception in operations in cyberspace. The latter is an attempt to manage anonymous attacks.

However, there are some areas where Russia is not keen on regulation. For instance, a proposal to regulate cyber-crime under a UN directive is still under consideration by the relevant Russian authority. One reason for the delay could be that many of the criminal activities conducted on a large scale worldwide originate from Russia or are connected directly or indirectly to the country. The infamous Russian Business Network, RBN, is said to be the mother of all cyber-crimes.[16] There is a suspicion that there are some connections between persons related to the Russian authorities and groups dealing with cyber-crime.

There are many areas to be addressed and resolved. An agreement on cyberspace will have to deal with issues such as censorship of the Internet, sovereignty, and how to handle rogue actors who might not be subject to a treaty. It must also include all forms of networked and digital activities not limited to the Internet and the cyberspace but also covering the overall field of electromagnetic pulse weapons and other related areas.

3.2 A Dual Approach. NATO and EU Outlook

Regarding the implementation of IW concepts, there are two international organizations that have to be included in this study – the European Union and NATO. In order to simplify their approach, I will only focus on the member states that are common to these organizations and have the most advanced information warfare doctrines and policies of implementation. These countries are Germany, France, and the United Kingdom. Before proceeding further, I would like to mention that in terms of approach to information warfare from the U.S. perspective I made reference in earlier chapters.

However, during the study, I will not let aside some essential steps that were achieved at the integrated level of both organizations.

Among the European countries, the first that has understood the need to develop IW policies was Germany. Starting with 2005, Germany has issued a national plan for information infrastructure protection that was perfected two years later and integrated into its *Critical Infrastructure Protection Implementation Plan*.

Still, there was a need to have a national strategy to cover the security into the information environment but that was partially implemented in 2011 when the German Ministry of the Interior published a security strategy regarding only the cyberspace. In this documented were included necessary measures to protect the critical information infrastructure by securing and strengthening IT systems, improving the framework for law enforcement and ensuring reliable information technology. Beyond all of these, the strategy also referred to the inherent training of the cyber workforce.

France had a similar vision to Germany in implementing national security strategies regarding cyberspace. In 2008, France released a White Paper on Defence and National Security. Underlining the emergence of cyber threats, this document stated that "*the French territory and population are vulnerable in new ways that must be now treated as key factors in adapting the defence and security. They are the results of direct threats to*

[15] Ibid

[16] O'Connell, K., *Internet Law: Russian company outed as mother of all cyber-crime,* 2007, available at http:
//www.ibls.com/internet_law_news_portal_view.aspx?id=1887&s=latestnews

France from…attacks on information and communication systems.” Also, during the presentation of this document, the French president at that time, Nicolas Sarkozy asserted that “*in terms of defence and security, control and protection of information is now real power factors”* and that “*cyber warfare has become a reality*.” In the same year, France launched a program to enable a better response to these new types of threats. That effort was deepened three years later, in 2011, when France issued a strategy regarding “*information systems defence and security”*[17]. Among other strategic objectives, the French major defensive interest was to secure the national ability to make critical decisions through the protection of information infrastructure, related to its sovereignty.

Unlike France and Germany, UK approach went further. Although based on the same need to secure the cyberspace, the principles to response to specific threats are more offensive. In June 2009, was published the Cyber Security Strategy of the UK[18], that developed a triple approach (see fig. 4) in order to provide information superiority in the cyberspace (risks mitigation, opportunities exploitation, and protection of information related to decision making). Closer to US doctrine, UK more recent[19] approach considers the importance of both offensive and defensive information methods in exploitation of information environment. These methods include Computer Network Actions (CNAs) and psychological operations. They are intended activities, focused on selected target audiences to achieve political and military goals by influencing behaviors and attitudes. Also, for military purposes, these actions are designed to weaken the will of the opponent part, reinforce the will of own supporters and gain the support of the uninvolved in order to prevail into the information battle space.

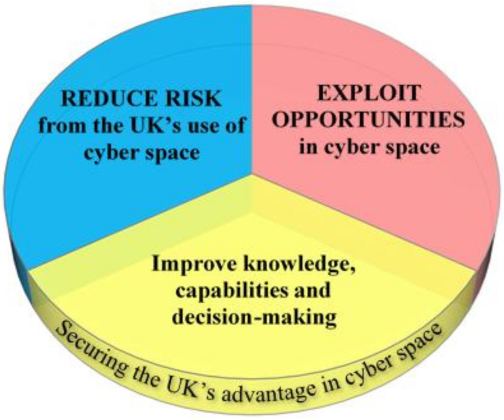
REDUCE RISK from the UK’s use of cyber space
EXPLOIT OPPORTUNITIES in cyber space
Improve knowledge, capabilities and decision-making
Securing the UK’s advantage in cyber space

Fig. 4 The triple approach in the UK Cyber Security Strategy (released in 2009)

At NATO level, a major step for promoting cyber security among member states was achieved in 2008 when the alliance set up a Cooperative Cyber Defence Centre of Excellence (CCDCOE), based in Tallinn, Estonia. One year later, an independent group of international experts was required by CCDCOE to develop a study project[20] regarding the legal framework related to Cyber Warfare.

[17] available on http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_ security _-_France_s_strategy.pdf

[18] available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf

[19] in a report dated September 2013 from the Financial Times, it is mentioned that UK develops a full-spectrum military cyber capability, including offensive assets

[20] *the Tallinn Manual on the International Law Applicable to Cyber Warfare* was released after three years of studying (2009-2012), Cambridge University Press, 2013

In 2012, a report called “NATO 2020”[21] asserted that NATO must “*accelerate efforts to respond to the danger of cyber-attacks by protecting its own communications and command systems, helping allies to improve their ability to prevent and recover from attacks, and developing an array of cyber defence capabilities aimed at effective detection and deterrence*”. Related to that, NATO has adopted a policy and an action plan in cyber defence, documents which were endorsed at the Wales Summit in September 2014. According to these, the top priority is the protection of the communications and information systems owned and operated by the alliance.

Meanwhile, in 2013, the European Union published its “Cyber Security Strategy: an open, safe and secure cyberspace”[22], a document that does not align with the NATO approach. Rather than promoting a collective effort in cyber defence, EU policy establishes a shared responsibility among member states to provide security and encourages them to develop and maintain their own cyber capabilities.

NATO, instead, has integrated cyber defence into the Smart Defence Initiative that enables member states to cooperate to develop and maintain capabilities they could not afford to achieve or procure alone. Some analysts assess that Smart Defence is intended to make EU more responsible in the future, as the US might withdraw its security forces from the European continent, a fact that could possibly lead to the North-Atlantic alliance breakup.

However, this is somehow an unrealistic anticipation. In the age of information globalization, there is no separation between continents and no country or power can expect to remain uncommitted. Consequently, it is as the former Secretary General of NATO, Anders Fogh Rasmussen told the leaders of member countries at 2012 Chicago Summit: “*together, we will keep NATO capable of responding to the security challenges of tomorrow, because no country, no continent can deal with them alone*”.

3.3 Hybrid Warfare. A military revolution or a revolution in the military?

In the past decade, some of the most important military forces and coalitions in the world, have tried to address and counter the so-called hybrid threats. The term “hybrid warfare” appeared at least as early as 2005 and was later used to describe the strategy used by Hezbollah in the Lebanon war in 2006. Since then, the term “hybrid” has dominated much of the discussion about the modern future war, to the point where it was adopted by military leaders and promoted as the basis for modern military strategies.

The issue at stake is that opponents are using conventional / unconventional, regular / irregular, overt / covert means, and exploit all sizes of war to combat Western superiority in conventional warfare. Hybrid threats are not limited to conventional means but they operate the “full spectrum” of modern warfare.

There is no question that opponents, past and present, have developed creative uses of the “full-spectrum” of warfare, including the use of regular and irregular tactics of war in all sizes. In total, this may well form a hybrid set of threats and strategies, but it is not clear why it should be used the term “hybrid”, in addition to its simple descriptive value.

In practice, any threat can be hybrid, as long as it is not limited to a single size and shape of the war. When any threat or use of force is defined as “hybrid”, the term loses its value and causes confusion rather than clarify the “reality” of modern warfare. Another problem with everything “hybrid” is that using a new term suggests that there is something

[21] see http://www.nato.int/cps/en/natohq/topics_85961.htm

[22] available at http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

new about modern warfare - while this may not be the case.

Most, if not all, conflicts in the human history were defined by using asymmetries exploiting your opponent's weaknesses, leading to complex situations involving regular / irregular and conventional / unconventional tactics. Similarly, the rise of cyber warfare have not fundamentally changed the nature of war, but its use has expanded into a new dimension.

At a recent event sponsored and organized by the Atlantic Council of NATO, the participants said that *"there is no generally accepted definition of terms related to hybrid war"*. In other words, the members of NATO cannot agree on a clear definition of what they are facing. How can NATO leaders expect to develop an effective military strategy if they cannot define what they believe is the real threat?

From this point of view, NATO, and other Western policymakers should forget all about "hybrid" and focus on the specificity and interconnection of the threat they are facing. Warfare, whether it is ancient or modern, hybrid or not, it is always complex and can hardly be subordinated to a single adjective. Any effective strategy should take into consideration this complex environment and find paths to explore without simplifying it.

However, there is hybrid warfare, no doubt, and it will be the future of war. Each state and ideally entire international community must embrace this uncertainty in its doctrine and policy. The current lack of legal and political means to address cyber operations make the international community vulnerable to these coordinated attacks. Because there is essentially no precedent addressing cyber warfare, most states stay away from the bad behavior of a nation directly addresses in cyberspace. If there had been a response to aggressive behavior within the Ukrainian network sphere, perhaps the West could have had a more convenient and cohesive response to the Russian invasion. As there are very few legally binding documents that would serve as guidelines when dealing cyber operations; there is not even a clear legal consensus whether or not accessing the system of an attacker is allowed.

The kinds of operations which Russia was conducting in Ukraine were not terribly new, or even sophisticated; rather, they exploit the fact that any operations in the cyberspace were confusing to Western nations. The ensuing debates leave them time and breathing space to continue their aggressive behavior.

In May 2014, Russian president V. Putin and president of China, Xi Jinping, had a common statement regarding the defence of the information space. This seemed to be more than a political declaration because five months later Fox News reported that Russia, China, and other Middle East powers (Iran) are waging unconventional warfare against other nations and NATO lacks a clear strategy to mitigate the threat. In the western view, the challenge was called *hybrid warfare* (see fig. 5), a combination of conventional, irregular and asymmetric means, including political-ideological manipulation techniques. The key issue here, which gained the entire media international attention throughout that year, was the Ukrainian crisis escalation, due to the Russian campaign to undermine the domestic stabilization efforts by supporting the armed separatist insurgency against the Ukrainian government.

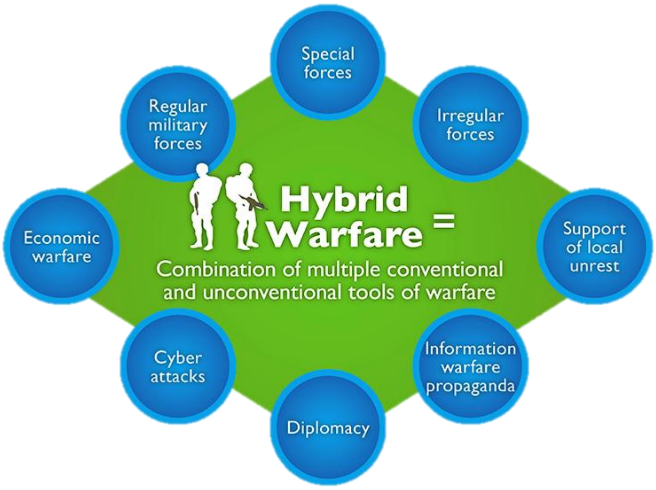

Fig. 5 Hybrid warfare diagram

In early 2014, a number of media reports provided by Reuters and other news agencies stated that Russian military forces used in Ukraine an advanced form of hybrid warfare that was heavily based on information operations.

It was reported, during the invasion of Crimea, that the local telecommunications networks were disrupted. The Ukrainian officials from the Ukrainian telecommunications company (Ukrtelecom JSC) said that a number of armed men have broken into their Crimean facilities and damaged fiber-optic cables. This cyber-attack was attributed to Russian military intelligence (GRU), as well as other activities that included attacks on government websites and social networks.

But this was only the local face of the Russian overall approach. To gain favorable international circumstances, Moscow has also used manipulation techniques through media to persuade the US and its European allies to manifest passive reactions and not to interfere with the Russian steps to dismount Ukraine through military and non-military means.

This type of information-based warfare Russians calls "*reflexive control*". It causes an adversary to choose the options that are most favorable to Russian objectives by modeling the adversary's perceptions over situation decisively. The Russian perspective on the use of IW differs from that held in West as it includes the undermining of political, economic and social stability through a massive psychological influence on the targeted population mixed with Special Forces operations in order to dismantle a nation and force the opposing state to take decisions that favor the Russian part.

As stated in the beginning, the Russian view on warfare is deeply rooted in the concept of the Soviet Union that was developed decades ago. However, I cannot agree that the idea of "reflexive control" lacks any theoretical innovation, as the global information environment through Internet was developed soon after the fall of Soviet Union.

In his article dated 27 February 2013, published in the weekly magazine "Military-Industrial Kurier", Russian general Valery Gerasimov[23] noticed that "*the information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy*. And referring to the Arabian Spring, he added that "*in north Africa, we witnessed the use of technologies for influencing state structures and the population with the help of*

[23] the current Chief of the General Staff of Russian Armed Forces, appointed by President Putin on 9 Nov 2012 It is believed that the Russian form of hybrid warfare is based on his vision called "Gerasimov Doctrine"

information networks. It is necessary to perfect activities in the information space, including the defence of our own objects."[24]

In Ukraine, the results of using asymmetrical means have been seen. Russia has prevented the West from intervening in Ukraine, allowing itself to build and expand its own military involvement in the conflict. Even more, it has created differences between NATO members about how to respond. However, due to the international economic sanctions, this approach has not gained domestic favorable attitudes among the popular or oligarchic views regarding Russian actions in Ukraine, and it has not created an information environment advantageous for Moscow.

Still, this doctrine of "reflexive control" should be properly studied by West, as the NATO approach, through its collective defence, provides a limited response to unconventional warfare. Securing the information environment, not only the cyberspace, at the alliance level, is a top priority and, also, an advance in the cooperation spectrum.

The majority of Russian attacks in cyberspace have been psychological in nature. The attacks were aided by the fact that over the past over 15 years, media has become more and more dominated by the state. This level of control internally, and within loyal Russian communities, has allowed for more psychological tactics such as playing on positive emotions by personifying soldiers and demonizing the West.

According to a NATO StratCom Center of Excellence report, Russia has been using social media as a platform for spreading disinformation and anti-Western feeling.[25] Information control is vital to the Russian strategy to maintain control of its citizens and prevent any dispute. In November 2014, Russia set up the government-controlled news site, Sputnik News, Dubbed by Foreign Policy the "Buzz Feed of propaganda."

Quite clearly, Russia has vast experience in spreading disinformation; and the West's traditional tactics cannot counter it. However, the omnipresence and accessibility of the internet provide an opportunity. Despite Russian attempts at limiting internet freedom, the Russian people still have the means to examine outside news sources to distinguish fact from fiction. Thus, trust in all media leaves the West's role in protecting the world order increasingly ambiguous, but certainly a free and open Internet can give citizens the opportunity to dig deeper, beyond the Kremlin's rhetoric.

4. Case Study: A More Comprehensive Look At Russia's Information Warfare In Ukraine

4.1 Concealing Information Warfare In Public Diplomacy

The Kremlin has been implementing a new strategic approach in Ukraine since February 2014 that depended intensely on Russia's concept of "information warfare." Russian information war was what the U.S. thought about it. It was, rather, part of Russia's method of conducting hybrid warfare, which consisted of an intentional misinformation campaign supported by actions of the intelligence agency designed to confuse the enemy and achieve a strategic advantage at low cost. The nature of hybrid operations made it very difficult to detect or even determine subsequently when they began, since confusing the

[24] see https://www.facebook.com/notes/robert-coalson/russian-military-doctrine-article-by-general-valery-gerasimov/10152184862563597/

[25] NATO StratCom Center of Excellence, *Analysis of Russia's Information Campaign Against Ukraine*, 2014

enemy and neutral observers were one of its essential components. It has become clear, however, that Russia was actively using its information warfare techniques and tactics in support of a hybrid warfare effort to reach its current objectives, intentionally the federalization of Ukraine or the concession of special legal status to the regions controlled by separatists in the eastern Ukraine.

In another context, Russia's action against eastern Ukraine and annexation of Crimea have become another area of Russia's testing of information warfare. The war has gained a multidimensional facet, being organized and inspired entirely by the Russian state. Using methods came to the Soviet times, Russia has managed to change the military intervention into a virtual conflict between Russia and the West (particularly the USA and NATO) building up the war's resources and facilities to lead a real "info war". Having resurged the old policy based on a rivalry with the United States, Russia has now unveiled its geopolitical ambitions and has imposed its way of thinking in terms of geopolitical blocs, while forcefully defining a border between the "Russian world" and the rest of the world. This has been the source of many difficulties and turns in Russia's relations with the West in recent history. Moreover, the West has not been able to formulate an effective response to Russia's revisionist policies, or find a way to support Ukraine as a victim of Russia's policy. [26].

Another aspect on the Russian "hybrid war" is that it is linked with the rising visibility of Russian broadcasting and efforts to shape public opinion around the world. Some feared that because information warfare was part of Russia's operations against Ukraine, other places where Russia's broadcasting and messaging have been felt may be future targets for "hybrid war" operations. In a lucky way for the West, there was a huge difference between Russia's worldwide broadcasting and public diplomacy goals and its operational goals in the post-Soviet space.

Russia did not create powerful state media institutions mostly to manage information warfare in Ukraine or any other post-Soviet country but it has invested huge resources in the infrastructure needed to get worse Western information control across the Internet and broadcast media. The goal was to interfere in control Western media sources and to break the public confidence in all types of institutions that Moscow viewed as being under Western, especially US, control, from international banks to the courts or governments.

Moscow wanted as much of the worldwide audience, and certainly its own people and those in the post-Soviet space, to question everything coming from the West. These efforts appear to have gained speed and power thanks to Russia's poor showing in international public opinion following the Russia-Georgia war of 2008, which proved how weak the Russian press was in comparison to the Western press. What many in the West seen as an effort to change people's opinions, adapted for the "hybrid war" in Ukraine, was in reality only one example of Russia's far wider and still changing global information strategy.

In its own version of "public diplomacy", Russia has turned information into a tool of national power and was using it to create room for itself and its interests in the international environment and worldwide public opinion. By seeding doubt, Moscow created space for maneuver for itself at home and abroad. In Ukraine, the first purpose of this tool of national power was to put in doubt the Western institutions and sources of information.

[26] Darczewska, J. *The information war on Ukraine - new challenges*, Cicero Foundation Great Debate Paper no. 14/08, 2014

4.2 The "True Face" Of Russia's IW against Ukraine

Russia's info war on Ukraine was taking place on the one hand internally, in Russia, and on the other hand externally, in the post-Soviet space. In the first area the main topic was: *"The West / the European Union is rotting, it's in decay, and the future belongs to the Eurasian Union"*. And in the global arena the argument was that *"a country as primitive as Ukraine cannot possibly be a partner for the EU or NATO"*. Russia's war was also taking place both in the real and virtual spaces and has involved several dimensions and aspects: while discredited the effectiveness of the Ukrainian leadership and prevented them from performing reforms, it attenuated Russia's image as an offender, presenting the Russian Federation as the state which *"strives to put down the fire and prevent a humanitarian catastrophe"*. Some specialists have in a wrong way confused info war with cyber war. The first term was much wider, even though it was an uncontested fact that foreign public forums were being flooded with significant amounts of pro-Russian posts and that software was being used in order to produce a viral marketing.

However, despite the difficulties to find the main features of this unusual and unexpected war regarding its scope, objectives, and main parameters, following characteristics of Russian aggression information can be identified:

- *There has been no formal declaration of war*, and the difference between the periods of war and peace was increasingly vague - the info war against Ukraine has been going on continuously since 2004 when the propaganda stereotypes such as the "orange plague" first emerged;

- *The absence of a single frontline* - it was a total war whose fronts might be located in one's own country and in any other country of the world, and your citizen might be the enemy while a foreigner might be an ally;

- *The information space was the main battlefield* - the aim of the psychological treatment was to instill fear, to the point of panic; the war propaganda found to weaken the enemy's morale and reinforce the morale of one's allies;

- *Efforts were made to mask the objectives and the official military engagement* - the point was to win without entering the fight;

- *Large groups of the public were being involved in the fight* – "defending Russians is a patriotic duty of citizens".[27]

On the tactical level, information warfare allowed Russia to achieve surprise in the time or manner of the attack. Russia thereby gained time and efficiency against the enemy's ground forces. Since, officially, the war in Ukraine was not declared, and the separatists conducted short high-intensity operations that limited the time that the United States had to respond before the situation went quiet, the enemy was usually taken by surprise and/or presented with an wrong or or fragmentary image of the situation. This factor has helped Russia's successful operation in Crimea with very few losses. The problem with that approach, though, is that as the West understands Russia's tactics better, the advantage of originality in Russia's approach to Crimea is less likely to profit its next venture.

The Informational cover provides more efficiency and flexibility to the military and improves the speed of maneuverability. For example, the initial rejection by the Russian chief commanders of the presence of the Russian soldiers in Crimea allowed Russia to gain time to take over strategic positions in Crimea. Since the start of the Crimean campaign,

[27] Darczewska, J. *The information war on Ukraine - new challenges*, Cicero Foundation Great Debate Paper no. 14/08, 2014

President Vladimir Putin repeatedly negated that the men in green uniforms were part of Russian Armed Forces, insisting they were groups of the local militia who had obtained their weapons from Ukrainians and even suggesting that they may have acquired their Russian uniforms from local shops.

Info wars were waged on visible and invisible fronts. The Kremlin defined the main frontlines, the secret services planners prepared individual operations, and the media carried them out along with the military, diplomats, experts, academics and representatives of the world of culture. Russian politicians readily embraced manipulation, disinformation, lobbying, lies and other methods of infamous propaganda. They denied any Russian military involvement in Donbas and said that the region had witnessed genocide and ethnic cleansing of those who wanted to speak their native language, rather than Ukrainian. *"The fact that today Donbas holds mass graves of murdered civilians proves this beyond any doubt"*, they said. The operations on the Western front was effective, as demonstrated by the experts and politicians who repeated the Kremlin's propaganda arguments *("One should find a solution that will allow Putin to save face"; Russia only demands respect and dialogue with the West on an equal footing")*. This was primarily a "war" of interpretations. Russia's interpretation was being reinforced and multiplied in all possible ways, while the "foreign" interpretation was being pushed to the margins where it posed no threat. The aim was to neutralize the enemy, support the allies and win over the undecided ones.

4.3 The "Hybrid" Aspect Of Russian Operations In Ukraine

Since February 2014 Russia has managed two separate phases of operations in Ukraine, beginning with the occupation and addition of Crimea, and continuing with the invasion of Eastern Ukraine's Donbas industrial area. Crimea began as a secret military operation, combining ambiguity, disinformation, and the element of surprise at the operational level with more traditional aids such as electronic warfare. The addition was completed by a traditional military invasion and occupation of the peninsula, using Russia's naval infantry, airborne, and motor rifle military units. This operation was like nothing else in the world, because Russia's Sevastopol naval base, the status of forces arrangements in Crimea, and additional agreements on the transit of troops in Ukraine enabled deployments and strategies that would not otherwise have been possible. These operations were, in that way, not easily reproducible in other places.

The Crimean policy was also separate within Ukraine, influenced by the Russian media in a manner other Russian minorities have not been. In recent surveys on public opinion and media viewership in Crimea, Professors John Laughlin and Gerard Toal have found that while the majority of ethnic Russians and Ukrainians in Crimea supported addition, the "*ratio of those who wanted to separate and join Russia definitely jumped due to television-fed perceptions that ethnic Russians would become second-class people in Ukraine"*. An important opinion of this polling, which suggests why Russian media proved effective, is that *"unlike residents of western and central Ukraine who tend to easily self-identify in these terms, the strong majority (85%) of the population of Crimea do not perceive themselves as European"*.

Russia's use of broadcasting tools for propaganda and psychological operations, part of a wider information campaign to support the Crimean addition, caught both Ukraine and the West by surprise. After its independence, Ukraine never argued over the information space in Russian language programming, such that Russian media, which had established complete control over the years, were able to quickly adjust their messaging in support of the Kremlin's goals.

The information warfare in Ukraine involved the planned-together use of Russian state-controlled media, but this was neither a new smaller part to Moscow's intervention in the post-Soviet space nor has it proven especially successful in the past.

During the 2004- 2005 Orange Revolution in Ukraine or the 2008 Russia-Georgia War, for example, Russia sent out and used information warfare tools, but to little obvious effect. Survey data from the past year proves that Russian broadcasting could not even convince parts of the Eastern Ukrainian population that had long been understanding of and willing to help Russia to support the separatist cause.

Moscow was surprised by the lack of positive response among the Russian-speaking Ukrainian population to its obvious media campaign against the Maidan protests and the interim government in Kyiv. Russia's direct military intervention in the Donbas was, therefore, necessary, at least in part, because of the apparent failure to motivate enough pro-Russian forces to sustain a wholly native rebellion.

It is an important element of the hybrid war to attach negative, emotionally charged labels to the enemy and promote them using all instruments available, knowing that one part of the public opinion will believe the labels, another part will get frightened by the possible consequences, and still another part, acting out of caution, will push the problem of Russian aggression to the margins of discourse.

What many in the West are identifying as the important buildup of Russia's “hybrid war” against Ukraine appears instead to be the unplanned series of different tools to fit different, often unexpected, operational realities.

4.4 A Quick Look To The Future

The information warfare and the conflict in Ukraine are by no means over. As a consequence, Russia will keep learning, and it is likely to come up in the future with more sophisticated informational tactics, even though the strategy failed to meet some of its goals. Among other approaches, it will keep using its Security Service very actively to influence Western decision-making.

However, recognizing the limitations of Russia’s hybrid warfare is as important as recognizing its power. Its success depends heavily on certain conditions holding in the minds of the adversary. The hybrid strategy will always rise significant challenges to the West, and it must be much more alert to the Russian attempts at reflexive control. But the West is not helpless in the face of such a strategy. It can and must, in fact, develop a theory and doctrine of its own to counter it.[28]

Hybrid war has become the catch-all term for the elements of national power. Given current tensions in and around Ukraine, which have resulted in a complete shortage of trust between Russia and its neighbors, fears that Moscow will continue to get involved in its vicinity are fully understandable. But a repetition of “hybrid war” is rather a wrong understanding of the problem. Ukraine is not the first example of a repeatable “hybrid war” doctrine, or of a strategy for projecting Russian power in the post-Soviet space and outside

[28] Kirchick, J., *How a U.S. Think Tank Fell for Putin*, The Daily Beast, July, 27, 2015, www.thedailybeast.com/articles/2015/07/27/how-a-u-s-think-tank-fell-for-putin.html

it. It is important to understand the combination of Moscow's tools, but the chances that it could simply repeat a Crimea or a Donbas scenario in other places are, fortunately, low.

Instead, Russia's intervention in Ukraine should be understood in more flexible terms as an attempt to employ diplomatic, economic, military, and information tools in a neighbor state where it perceives very important national interests to be in danger of being lost. This could be a framework for the use of national power which the U.S. itself should find familiar, and equally concerning.

Looking forward, the most important question for policymakers will remain, not what are the features of “hybrid war” or any other supposed model of warfare, but rather how to deal with a major power such as Russia when it chooses to employ its full range of power. The US response will prove not only important to the result of the current confrontation and future conflicts on Russia's edges, but it will also shape global and regional challenges to be faced with other major powers in the coming years.

5. Conclusion

We live in the information age when the overall environment is increasingly changing faster and demands major adaptive reactions from any social actors – individuals, organizations or nations. Already so far, through the global interconnection, most of our privacy was lost in exchange for gaining access to the open world. Our society has become highly dependent on information technology in each area from our lives. Today we have communications satellites, computer networks, fiber optics, smartphones and tablet computers that allow us to reach anywhere almost instantly. But in the same way, in just a few seconds, our information can be intercepted, distorted or stolen.

The problem is that the rapid change of information environment cannot provide effective ways to counteract new types of information attacks. From this reason, the bureaucracy has no place in an information warfare environment where attacks are conducted in seconds and reactions must be alike.

Somehow, we have left behind the critical needs to comprehend, secure and actively manage our information environment as much as we transition to the *knowledge age*. Nowadays, there is an explosion of brainpower in many top disciplines of science and technology (genetics, robotics, nanotechnology, etc.) that remains outside of the military, intelligence services and law enforcement agencies. This could imply a serious risk to individuals, organizations and nations if this capital is not properly secured and fall into the hands of hostile states or non-state actors.

Still, there are more challenges to face due to the information globalization. It is a true fact that, nowadays, information itself is seen as a valuable resource. In economic terms, it means that *gaining access to secured information on resources is equal to gaining control of resources.* Hence, the competition for resources has become a competition for *information on resources.* Instead, in the world of corporations, *sharing information on secured resources does not mean sharing control on resources.* Consequently, the competition is more encouraged than cooperation and the information warfare has become a sufficient means to cancel the difference between peace and war.

Yet, this confrontation has visible traces in our daily life. As the overall population grows rapidly, many of resources become scarce due to the unequal distribution or concentration of them into the hands of few owners. The request for energy is rising exponentially and generates more dependencies between providers and new customers, which means that the information infrastructure is continuously expanding. The global economy is estimated to grow significantly, thus in 2020 it is projected to be around 80%

broader than it was in 2000. More companies will become global and will reach such level of power and influence throughout the world that even superpowers cannot easily deny it.

Many nation-states are already, entirely dependent on corporations for their national information infrastructure and the evolution of environment makes that these companies have become part of the critical national infrastructure. Ironically, these corporations are in the best position to interrupt or disrupt for some reasons the proper function of some industrial facilities or other key infrastructure. So, in this case, *dependency means vulnerability*.

Furthermore, we have seen in the last years the rise of criminal and terrorist organizations that were able to penetrate, gather intelligence and sabotage critical security facilities by carrying out coordinated inside-the-wire attacks. They possess sophisticated information technology and engage in asymmetric warfare against the most exposed targets when lacking the capacity to confront in the traditional battlespace.

Also, the use of the Internet by terrorists is not recent. In the past, we have witnessed how they gather funds, communicate and promote ideological propaganda, psychological influence. But with the emergence of Islamic terrorist groups such as Al-Qaeda and ISIS, there has been a significant increase in the use of social media. Particularly, ISIS has demonstrated a considerable understanding of its power and has achieved great effects in its recruitment campaign.

Clearly, surpassing all the other global stakeholders, remain superpowers as the main actors in the arena. They cannot give up their power and influence in the open world since information warfare is the best tool to sustain them. And through it, they still compete for supremacy as in the Cold War.

Perhaps in the future, depending on the evolution of technology, superpowers might achieve powerful information weapons that will be considered among strategic deterrence capabilities. But until then, the global information infrastructure will gain virtually and physically new dimensions and, probably, will definitely move the effort on securing the information environment into space.

References:

[1] *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space*, 2011, https://ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf;

[2] *Cyber-crime Cyberterrorism Cyberwarfare Averting an Electronic Waterloo, CSIS Task Force Report, Center for Strategic and International Studies,* 1998, Washington DC;

[3] Ballantyne, G., *RUSI Newsbrief,* published in Issues in Science and Technology, 1998, www.terrorism.now;

[4] Darczewska, J. *The information war on Ukraine - new challenges*, Cicero Foundation Great Debate Paper, no. 14/08, 2014, http://www.cicerofoundation.org/lectures/Jolanta_Darczewska_Info_War_Ukraine.pdf;

[5] Hunter, E., *The Challenges of Hybrid Warfare,* International Centre for Defence Security, Estonia, 2015;

[6] Kirchick, J., *How a U.S. Think Tank Fell for Putin*, The Daily Beast, 2015, www.thedaily beast.com/articles/2015/07/27/how-a-u-s-think-tank-fell-for-putin.html;

[7] Kofman, M., Rojanski, M., *A closer look at Russia's hybrid war*, published in Kennan Cable, no 7/2015, https://www.yumpu.com/en/document/view/55318947/a-closer-look-at-russias-hybrid-war/7;

[8] O'Connell, K., *Internet Law: Russian company outed as mother of all cyber-crime,* 2007, http://www.ibls.com/internet_law_news_portal_view.aspx?id=1887&s=latestnews;

[9] Valeri, L, *Information requirements for Information warfare: the need for a multidisciplinary approach,* 1999, London;

[10] Schwartau, W, *Information warfare: Chaos on the Electronic Superhighway*, Thunder's Mouth Press, 1994, New York;

[11] *US Joint Publication 3-13, Joint Doctrine for Information Operations*, http://www. dtic. mil/doctrine/new_pubs/jp3_13.pdf;

[12] *https://www.facebook.com/notes/robert-coalson/russian-military-doctrine-article-by-general-valery-gerasimov/10152184862563597/*;

[13] *http://www.sras.org/military_doctrine_russian_federation_2010*;

[14] *http://www.nato.int/docu/Review/2015/Also-in-2015/hybrid_modern_future_warfare_Russia_ukraine/EN/index.htm*;

[15] *http://www.nato.int/cps/en/natohq/topics_85961.htm*;

[16] *http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf*;

[17] *http://www.thelivingmoon.comnthelivingmoon.comnzorgon.thelivingmoon.com/91_PDF_Database/US_Air_Force_2025/vol3ch03.pdf*;

[18] *http://www.qcert.org/sites/default/files/public/documents/GER-PL-CIP%20Implementation %20Plan-Eng-2007.pdf*;

[19] *https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?_blob=publicationFile*;

[20] *http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence _and_security_-_France_s_strategy.pdf*;

[21] *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf*;

[22] *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/486301/20151210-Archived_DCDC_FCOC.pdf*;