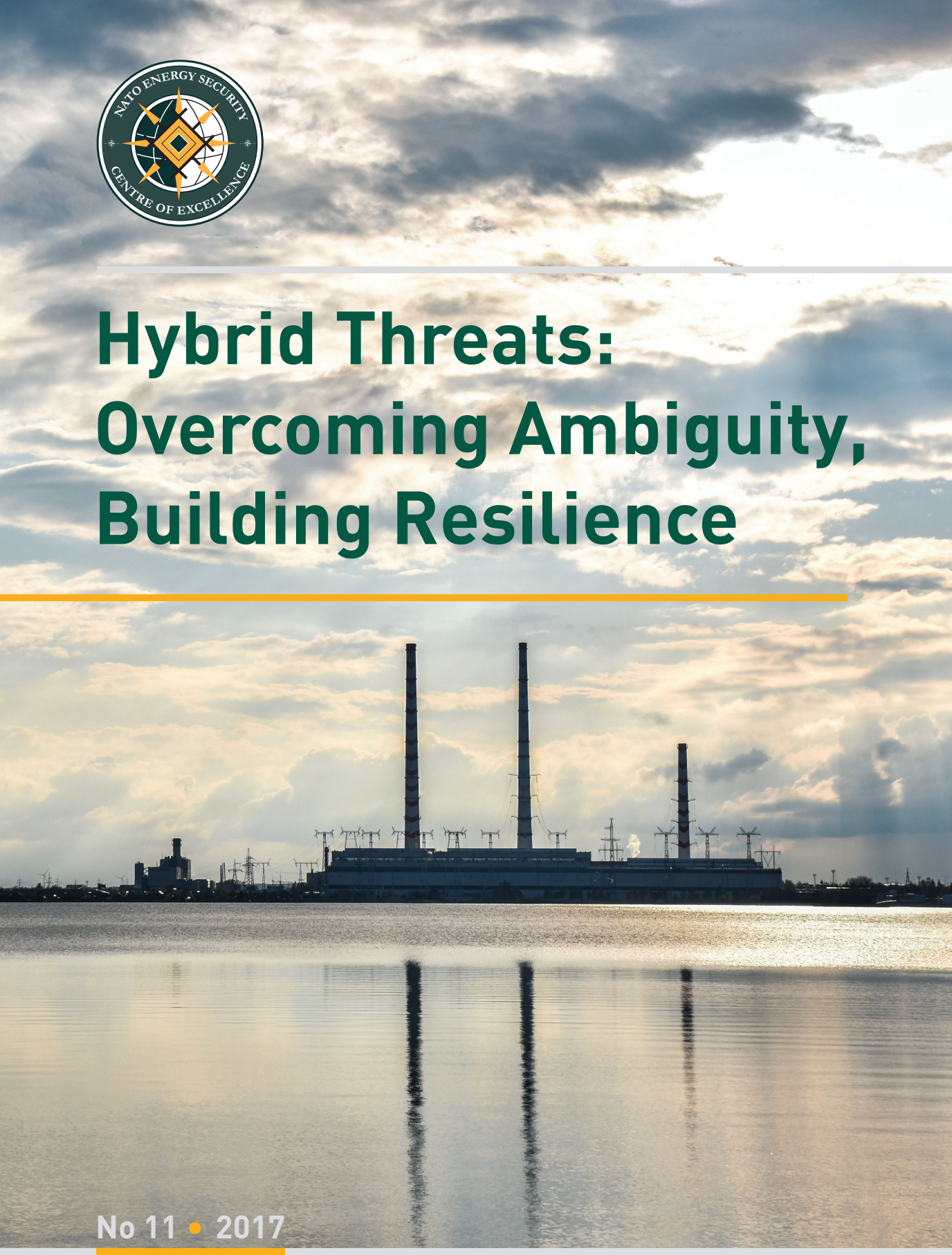

Hybrid Threats: Overcoming Ambiguity, Building Resilience

No 11 • 2017

Contents

Editorial

Dr. Jaroslav Hajek
Subject Matter Expert
Strategic Analysis and Research Division, NATO ENSEC COE

On 10th-11th September 2015, NATO Energy Centre of Excellence (ENSEC COE) organized a workshop entitled "Hybrid threats: overcoming ambiguity, building resilience" in cooperation with the Institute of International Relations and Political Science of the Vilnius University and the Ministry of Foreign Affairs of Lithuania.

The aim of the workshop was to discuss security issues in Eastern Europe and lessons learned from the Ukrainian crisis. The event brought together leading experts from NATO and national bodies, academic scientists, researchers and media representatives who exchanged their experiences and their perspectives on hybrid threats and their prevention, as well as on energy security issues and critical energy infrastructure protection. The workshop provided a platform who profitably contributed to raising awareness about security issues and hybrid threats and to increasing knowledge on countering misinformation, deconstructing propaganda and dealing with ambiguity. This was also a valuable contribution for exchanging practical insights about the ways of improving EU's and NATO's instruments for coping with hybrid threats.

In order to spread the good results achieved, NATO ENSEC COE has decided to publish this issue which contains eight selected texts. Major General Edvardas Mažeikis focuses his keynote speech on hybrid war. He provides valuable examples and explains the difference between past and present hybrid war while presenting the necessary measures to countering hybrid threats. Deputy Director of NATO Strategic Communication Centre of Excellence (StratCom COE) Colonel Aivar Jaeski highlights the fundamental role played by NATO COEs in helping the Alliance to deal with the new security environment since the collapse of the Iron Curtain. He discusses in particular one of the several studies conducted by NATO StratCom COE which analyses, inter alia, two of the most dangerous information campaigns conducted today, namely Daesh's Information Campaign and Putin's Propaganda Campaign against the Western world. Political Advisor in NATO Land Component Command Heidi Meyer's article discusses some measures that NATO should consider taking up to adapt to ambiguous threats so that decision-making is not so challenging and political and military responses are at the right level and at the right time. Research Director of the Ecole Militaire Strategic Research Institute (IRSEM) of the French Ministry of Defence Christophe-Alexandre Paillard analyses the key energy challenges that the members of the EU and the European members of NATO have to face. In doing so, he specifically focuses on the Middle East and Northern Africa (MENA) area. Ambassador-at-Large for Energy Security in the Czech Republic Vaclav Bartuška assesses the European energy security in the stand-off with Russia in 2014-2015. Executive Director of the Centre for Global Studies Andrii Chubyk and President of the Centre for Global Studies "Strategy XXI" Mychailo Gonchar analyse the energy component in New Generation Warfare with a focus on the Russian hybrid war against Ukraine. Head of Energy Security and Technogenic Safety Department of the National Institute for Strategic Studies Oleksandr Sukhodolia describes energy dimension of hybrid warfare against the Ukrainian critical energy infrastructure. Co-founder and CTO/Head of epitaxy of Brolis Semiconductors Kristijonas Vizbaras' article discusses the volunteer militia organisation "Lithuanian Riflemen's Union" (LRU), which has attracted many members as a reaction to the Russian annexation of Crimea in 2014 and which is the most important organization of its kind.

Keynote Speech

Maj. Gen. Edvardas Mažeikis,
NATO Standardization Office, Belgium

Before I start talking about hybrid threats, I would like to ask you: Are the means and methods used for hybrid warfare new? Is the definition of 'hybrid warfare' new or old? Of course, it is as old one like the Earth and the wars on it. I can name one of the typical hybrid warfare examples from ancient times: the story of the "Trojan horse", when Greeks constructed a giant wooden horse with soldiers in it to enter the city of Troy. Also, at the beginning of II WW, with the attack on Poland, the Winter War with Finland in 1939 or the so called casus belli, which started the war, can be treated as hybrid warfare as well. The Nazis organized an attack on their own radio station by a group of people dressed in polish uniforms. The Soviet Union organized the shelling of its own border guard post (4 killed, 9 injured) at the Finnish - Soviet border and later blamed the Finns. After the war started, they immediately organized a puppet government for Finland headed by Otto Wilhelm Kuusinen.

A more recent and geographically closer example of hybrid attack is the Bronze Soldier monument relocation in Estonia in April 2007. This can be seen as a quite modern approach to hybrid warfare. Riots during the known Bronze Nights in Tallinn were orchestrated and organised by a group of people all looking alike, having short haircuts and civilian black jackets. The besieging of the Estonian embassy in Moscow for a week and cyber-attacks on Estonian organizations are examples of continuing steps of hybrid warfare used against Estonia. Therefore, looking at the historical view of hybrid warfare, I can say that lying and cheating have always been a basis for hybrid war. The number of activities conducted by the USSR throughout the Cold War might now be described as a hybrid threat. The Soviets secretly participated in many regional wars, amongst others, the wars in Vietnam, Korea, the Middle East and Africa in which different specialists and frontline fighters such as pilots, air defenders and so on were used, without a clear national identity shown on their uniforms.

What is the main difference between past and present hybrid war? Today the information

Maj. Gen. Edvardas Mažeikis, NATO Standardization Office, Brussels

Maj. Gen. Edvardas Mažeikis took over the position of Director of the NATO Standardization Office on 1st July 2014. Previously, he served as Commander of the Lithuanian Air Force and as Chief of Defence Staff at the Ministry of National Defence. Here, he ran the Defence Capabilities Planning Department and Armaments and the Communication Systems Department. Between 2008 and 2010, Maj. Gen. Edvardas Mažeikis served as Commandant of the Lithuanian Military Academy. From 2004 to 2008 he had been appointed as Lithuanian Military Representative to NATO and to the EU Military Committees in Brussels. In 2007 he was nominated Dean of NATO Military Committee for one-year. From 2000 to 2004 he was the first one to serve as Commanding Officer of Lithuanian Air Force with the aim to reform the Air Force to meet the requirements of NATO membership.

service has become a hybrid combat service in some states or terrorist organizations. The Russian President Putin awarded a group of "news makers" belonging to the Russian propaganda machine after the Crimea campaign with high level state awards. They were addressed with the pseudo 'funny' term "information troops" (*informacyonnye vojska*). As Russians like to say: each joke contains just a part of the joke – the rest is true. Information wars today have become as important as a real artillery shelling on an enemy position. Manipulating of information is at the heart of hybrid strategies. For a regime without any moral limits (in western understanding), being it Russia with its leadership's criminal mentality or Islamic State of Iraq and the Levant (ISIL) with its terrorist mentality, lying and cheating is not a problem at all.

Another modern hybrid threat is cyber-attack. With limits placed on tracing the origin of the attacker, being relatively cheap yet quite effective, it fits in very well with the hybrid threat definition.

As I started talking about modern hybrid threats, I would like to read the clear definitions which we are using in the Alliance. It is my duty as Director NSO, because we are also responsible for the terminology and the agreed language in NATO.

Hybrid strategy: A comprehensive strategy to achieve (geo)political and strategic objectives based on a broad, complex, adaptive and often highly integrated combination of conventional and/or unconventional means, overt and/or covert activities, military, paramilitary, irregular and/or civilian actors, conducted across the full spectrum of elements of power (diplomatic/political, information, military, economic, financial, intelligence, legal – DIMEFIL) intended to create ambiguity and targeted at an adversary's weaknesses and vulnerabilities. Hybrid strategies have a particular focus on decision-making process.

Hybrid threat: A state or a non-state actor that has the capacity and apparent willingness to employ a hybrid strategy. A hybrid threat is manifested in activities that fall short of direct conventional military action and that can be conducted for extended periods of time.

Russia is the primary practitioner of hybrid warfare. It has a great deal of experience in using it if we take this country as the main successor of the Soviet Union. Other actors including terrorist organisations have pursued hybrid strategies, too. Simultaneous, opportunistic, synergistic and sophisticated combination of conventional, irregular and criminal/corrupt actions in designated geographical areas to achieve political aims is common to state and non-state models.

Russia's approach seeks to create ambiguity aiming at blurring the distinction between war and peace and at concealing the instigator's role as a party in the conflict. This latter is a key element in undermining the decision-making and in weakening the effects of the tools available for a response in the nations targeted and governed by the consensus organizations.

Both Russia and Daesh (ISIL) are now engaged in hybrid warfare against their perceived adversaries. The possibility to use an overt military action as part of the hybrid strategy cannot be discounted. Russia has not employed a hybrid strategy against Ukraine alone. Rather it has adopted a hybrid model that targets Ukraine and the nations and organizations that Russia sees as opponents to its global aims and interests. Similarly, Daesh's approach focuses on individuals as well as on nations and international organizations.

Discussions about hybrid threats started immediately after the 2014 Wales Summit. RAP (Readiness Action Plan) is central to NATO's ability to counter all threats including hybrid ones. Findings about hybrid threats and how

to counter them will be reflected in the process of new doctrine development. The Alliance is in the position today that all main doctrines should be revised. This is a normal procedure carried out every three years. But this time is special, because of the Alliance's centre of gravity shift from Counter insurgency operations (Afghanistan) to Article 5 activities. The NSO is starting an Allied Joint Doctrine Campaign together with all NATO Member Nations and main Alliance commands, where ACT is playing a very important role.

The possibility to be proactive depends very much on the possibility of receiving warnings and indicators regarding incoming actions. Activities in the context of Confidence and Security Building Measures (CSBM) and arms control can contribute to providing warning indicators. In the case of hybrid threat warning, indicators and monitoring are the most important basis for decision-making. Decision-making is really difficult when the line between war and peace is blurred, like in the case of a cyber-attack.

Civilian/political actions should be taken immediately, even before the possibility of military response, when the warnings and indicators show the hybrid campaign has been launched against a nation. In his interview to the mass media, an Estonian general talked about the possible reaction to an invasion of the so called "green men": shoot the first "green man" who crossed the state border and the issue would be solved quickly. In the Baltic nations, the well-known British journalist Edward Lucas agreed in one of his articles that sometimes it can be effective. At the same time, what if instead of the "green man" with a weapon in his hands there was a 15 year old Russian speaking girl participating in aggressive demonstrations against NATO, the EU or the Estonian Armed Forces in Narva (which is close to the eastern state border, where the overwhelming majority of Russian speaking population is living in Estonia)? Then the principle "shoot first – think later" does not work.

In the early stages of a hybrid campaign, the actions targeted against nations are likely to principally constitute an internal security challenge. It is therefore the nations to be threaten by such a campaign that should have the primary responsibility in responding. The requirement is for a 'whole of government' response that combines all national instruments as part of a national plan. This plan can foresee an option for a nation to turn to the Allies and the wider international community for assistance. International organizations (NATO, EU, OSCE and UN) can be effective but the assistance should be coordinated by the receiving national authorities in concert with their national plan for countering the challenge they face. First and very important: effective analysis and early recognition based on intelligence and information gathering from different sources.

Measures can be described by three words: Prepare, Deter, Defend. These are not necessarily sequential activities, but functions that may have to be undertaken simultaneously to ensure resilience and an effective response against hybrid threats, depending on how a hybrid campaign is applied and evolves.

PREPARE:

Building resilience. Hybrid strategies seek to find and exploit vulnerabilities in the target nation and the international organization. At the national level, effective resilience would include a coherent and up to date national crisis organization, developed security and defence structures, and capabilities and civil preparedness. Respected and transparent governance is also very important. Cyber resilience is very essential as well.

Comprehensive analysis. At the national and the international level, accurate and timely shared intelligence information supported by comprehensive analysis are fundamental to the identification of hybrid threats, to the recognition of their employment and to the anticipation of the need to react to them.

DETER:

The requirement is for the 'whole of government' response that combines all national instruments as part of a national plan. Military and civilian preparedness postures and means are complementary. From NATO's perspective, strong political will and Allies solidarity, including visible military deterrence, will contribute to deterring a hybrid campaign. Capability and readiness to deploy forces quickly and Alliance responsiveness, including effective and timely decision making, are key to achieving a credible deterrence.

DEFEND:

A Nation under attack can be supported by the means of Article 5. But blurred lines between war and peace in the case of a cyber-attack for example, or a combination of protracted and indirect conflict, a blend of lethality, coercion and intimidation helps an aggressor conceal and deny his real intentions. This requires support and assistance from NATO and the EU much earlier. Allied nations can request the deployment of the rapid reaction forces in response to a deteriorating situation.

Generals are normally blamed for preparing for the previous war. Just to try and change this old impression slightly, I would like to talk about the future.

FFAO (Future Framework Alliance Operations) is a new document developed at ACO. It is currently being discussed by Allied Nations and different NATO committees. It says the following about emerging technologies: emerging technology will provide many opportunities for the Alliance, but it will create significant challenges as nations and non-state actors seek to narrow NATO's current technological advantage. Allied forces will need to understand technology and be able to innovate new and creative tactics, techniques, procedures, capabilities and doctrine. The Alliance will need to be cognizant of the acquisition and innovative use of technology by others. Without incurred cost of research and development, nations and non-state actors can capitalise on technological advancements and translate them into capabilities that threaten the Alliance. While it is impossible to predict all the areas where technology could revolutionize warfare, some of the key areas to monitor include: directed energy, autonomous systems and sensors, quantum computing, unmanned systems, electromagnetically launched projectiles, renewable energy, artificial intelligence, 3D printing, additive manufacturing, biotechnology and nanotechnology.

When we discuss overcoming ambiguities and building resilience for future hybrid threats, we have to keep in mind that the tool box creating such threats is very large, and continually growing larger.

What to do with hostile information campaign/propaganda?

Col. Aivar Jaeski,
Estonian Defence Forces, Estonia

The North Atlantic Treaty Organization (NATO) as a defensive alliance uniting 28 members effectively communicates the intention to protect its members. It spreads this message not only through speeches, articles and videos, but also through actions such as the rise of force posture, the establishment of new headquarters, and the increase of airpower presence and exercises.

How effectively NATO as a collective organisation handles the new security environment depends on each single nation out of 28. The chain constituted by the member states is NATO's strongest and weakest characteristic at the same time. National positions are often driven from geographical location, economic development and historical experience. A single country cannot gain knowledge by ignoring the wisdom already gathered. It is hard to get an objective assessment only relying on one source or one perspective. The collective effort always provides better results. Therefore, NATO creates collective multinational establishments.

Since the collapse of the iron curtain, NATO has been flexibly adapting to the new security environment. The Partnership for Peace programme, the enlargement process, and programs aiming at helping earthquake victims are just some examples of its past endeavours. Today, the main threats on the Alliance's nations come from Hybrid Warfare, which includes areas such as cyber space, energy and communication. With the help of the Centres of Excellences, the Alliance thoroughly studies those threats. Multinational NATO Centres of Excellence provide a unique opportunity to bring together the collective knowledge and experiences of the Alliance's nations and partners by translating them into proposals to enhance NATO's processes and capabilities.

Col. Aivar Jaeski, Estonian Defence Forces, Tallinn

Col. Aivar Jaeski joined the Estonian Defence Forces in 1992. He has served in the Armed forces as platoon leader, company commander and battalion commander. Col. Jaeski has been also commanding officer of the Estonian Peace Operation Centre (EPOC), responsible for training soldiers for international missions.

In 2003, he was appointed Deputy Military Representative (DEPMILREP) at Estonian Delegation to NATO Headquarters (HQ) in Belgium. Col. Jaeski has also served as defence planning section head of the Estonian General Staff J5/9 (planning) branch. In 2009, he was appointed as Section Head of the Information Influence Section of the Operational Directorate Joint Effects Management Branch of NATO Joint Forces Command Brunssum (JFCB). In the autumn of 2012, Col. Jaeski worked as Chief of the Public Relations Department of the Estonian Defence Forces HQ, which he changed into Strategic Communications Department. Since the 1st October 2014, Col. Aivar Jaeski has been working as Deputy Director of NATO Strategic Communication Centre of Excellence. Additionally, Col. Jaeski has accomplished several missions in Iraq and Afghanistan.

NATO Strategic Communication Centre of Excellence (StratCom COE) finalised several studies at the end of 2015. Important ones covered, inter alia, the most dangerous information campaigns which are being conducted today, namely the DAESH's[1] Information Campaign and Putin's Propaganda Campaign against the Western world.

In this regard, I will now present a comparison between these two campaigns and a conclusion with recommendations for NATO's decision- makers, nations and partners. I will also provide some food for thought to people who are interested in these issues.

The NATO StratCom COE's studies on the DAESH's Information Campaign and Putin's Propaganda Campaign have discovered several common issues between them. Firstly, their main goal is to get a dominant position in the world, if not in the whole globe, then for sure in a certain region.

The study of the audiences of DAESH, which has been conducted by grouping the messages that it receives, has allowed us to identify four lines of effort which serve the main objective. Those lines are Support, Unite, Frighten and Inform.

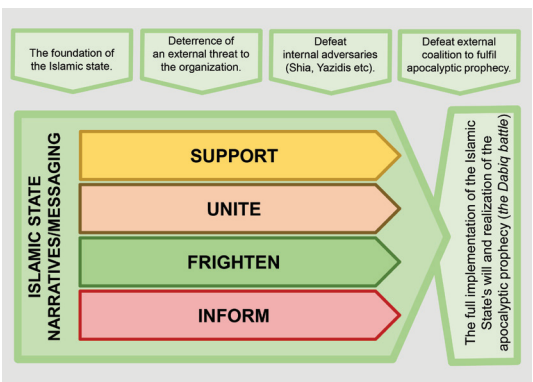

Figure 1. DAESH Information Campaign

In order to support those lines of effort, the organisation does not only focus on the personnel (fighters/foreign fighters), but also on the financial, military, energy, and informational tools such as leaders' announcements, writing on online media etc.

Through communication, DAESH supports everybody interested in joining their ranks. Their messages are well thought and structured: they call the muslim believers (young people in particular) for joining their army in order to become soldiers of truth. They justify their organisation's violent actions by stating that there is no life without Jihad.

With a united effort, DAESH uses the promises of a prosperous life and of a better administration, which is something people do not have today. Showing people pictures of a "normal" life, of law and order under the rule of Islam works as a recruitment tool for families who live a difficult life. In this context, the name 'Islamic State', which is used by terrorists, is powerful and influential.

A frightening line of effort works towards both external and internal communities. Terrorists engage common people to reach their goals by putting words into action and by sharing their ambitions with them.

Looking DAESH's Informing line of effort, we can see that it uses tools (magazines, radio broadcasts, TV stories) similar to those used in developed countries. They are particularly active in social media, which deliver information very quickly and address a wide audience.

All those lines of effort were conducted when and where so called Islamic State was announced at first, the external threat recognised and the defeat of their internal adversaries started. The next step to defeat external adversaries has already been initiated.

When we look at Putin's regime propaganda campaign against the Western world, we can observe similarities with the DAESH's lines

[1] Mass media sometimes refer to Daesh with the name ISIL or Islamic State.
[2] The Guardian, Vladimir Putin's approval rating at record levels, available at http://www.theguardian.com/world/datablog/2015/jul/23/vladimir-putins-approval-rating-at-record-levels

of effort. Like DAESH, Putin wants to gather supporters for his path towards a dominant position in the international arena. Today, we can see that Putin's regime has internally succeded. According to "The Guardian", in Russia 87% of the population trusts President Putin's actions[2]. Besides the massive use of media tools, we have also seen the great support of the Russian Orthodox Church for the regime.

Outside Russia, Putin's regime does not look too much for external support. According to the PEW Research Centre's Attitudes Survey, he only has over 50% support from Vietnam and China. The average trust in his actions from abroad is 24%. His arrogant attitude has driven President Putin's position to be a regional player who does not need international cooperation, external wisdom and advice.

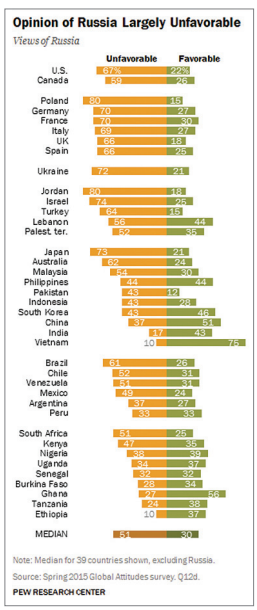

Figure 2. Little confidence in Putin

Therefore, instead of looking for cooperation, the Kremlin puts more emphasis on means that create confusion and undermine the existing democratic system in the West and its values. This is achieved by falsifying historical and real life facts and by influencing the public opinion through social media with the help of the 'troll farms' and of conspiracy theories developed ad hoc. Names like Novorussia, used by separatists and advertised by the Kremlin, have influenced and motivated many Russians to voluntarily go to Ukraine to fight against the fascists.

The Kremlin's violent rhetoric is driven from the will to scare people, and is used by Russian convicts who argue that *"боится значит уважает"*, meaning "if you are scared of me, you respect me". In this context, Putin makes huge efforts to demonstrate Russia's superiority. The wars in Georgia and Ukraine, the annexation of Crimea, the flights of old Russian nuclear bombers, the opening of the new Arctic Joint Strategic Command are just examples of military force aiming at showing Russia's strength. Additionally, diplomatic and economic tools are also exploited together with the cyber domain.

Russia has large natural resources available. Energy resources and other natural raw materials have also been used as tools by the Kremlin to influence neighboring countries.

While DAESH is just building its communication capabilities, Putin's regime has managed to take control of the media inside Russia. At the same time, it has invested in external tools like the TV channel "Russia Today" RT), and online media projects such as "Sputnic". They now are the main tools to influence the West.

What are the conclusions of this comparison? Why have not those regimes collapsed yet? Why does their propaganda even affect our democratic countries?

Firstly, both DAESH's and Putin's regime know their audiences very well. They know whom to address and how to send their messages efficiently.

Secondly, "the name" of the terrorist organisation or separatist built state has a strategic meaning. Relating yourself with something big always has a significance in people's minds.

Thirdly, they carefully select facts and information to support their own propaganda campaign. Most of the time, those facts contradict the truth, since conspiracy theories are built and history is falsified.

Fourthly, religion as a powerful tool is brought into the game by both players.

Fifthly, recruitment campaigns are effectively organized by using powerful symbols and names.

Sixthly, the well-known fact that every communicator should know is that "actions speak louder than words".

Seventhly, for both DAESH and the Kremlin there are no limitations or restrictions for conducting their campaigns. Their goal is to challenge the free speech and abuse it.

This said, the list of recommendations of what can be done is quite long. Therefore, in order to help understand it better, we have grouped our proposals by using the PMESII (Political, Military, Economic, Social, Infrastructure and Information) domain.

In the political domain, we should not become part of their information campaign – we should choose words and actions carefully. We also should: revise the policies that are delaying the effective recognition of threats and hampering fast decision-making processes; support free speech in areas and countries where it is needed; unite people/organisation/countries to fight against the adversaries; conduct strategic communication! Speak out. What is obvious for some, is new for others.

In the military domain, we need: to invest in capabilities and deterrence; to study the information environment and rise situational awareness; to share, coordinate and cooperate; to allow others to use our capabilities for situational awareness and analysis, avoid duplication; to prepare for the worst case scenario - practice! Practice not only crisis response operations, but also conventional conflicts.

In the economic domain, it is necessary: to implement economic sanctions against adversaries and advertise them globally; to become independent from energy sources and raw materials coming from adversaries; not to conduct business or trade with adversaries; to close our financial system to adversaries.

In the social domain, we should: educate the population and learn from history: the newly discovered is often the forgotten old; build social awareness on adversaries' propaganda campaign, and report every offensive message and messages which are leading to radicalization, especially in Social Media; refine and protect audiences who can be vulnerable to the adversaries' propaganda campaign.

In the infrastructure domain, it is important: to invest in supporting structures like communication capabilities, situational awareness capabilities, education facilities, as well as deterrence infrastructures such as military bases and training facilities; to find alternative structures for delivering energy supplies. A good example is the Lithuanian investment into the Liquefied National Gas (LNG) terminal in order to be independent from Russian gas suppliers.

In the information domain, we should: draw particular attention to the quality of mass media; educate reporters to be truthful and to be able to recognise propaganda; maintain close cooperation with Social Media corporations in order to remove extremism from Social Media platforms; reveal lies, care about the truth; use legal tools and be proactive, cooperate; find a balance between reactive and proactive media. With new communication platforms (social media), where news and ideas are exchanged much faster, lies are also spread much quicker.

Finally, taking into account all those recomended "should", what do we have to keep in mind? Firstly, we should remember that not every Islamic organisation supports DAESH, not every Russian supports Putin's regime. Secondly, social media, national webpages and mass media are responsible for publication. This should not be taken for granted when hate speeches and lies appear in the media. The available legal means should be used in order to protect our societies. And last, but not least, there are organisations that oppose DAESH's and Putin's regime. In so doing, they diminish the influence of these latter's propaganda on target audiences. We must cooperate and support them.

A NATO Land Domain **Perspective**

Ms. Heidi Meyer,
NATO Allied LAND COMMAND, Turkey

INTRODUCTION:

The Euro-Atlantic region is dealing with a changed security environment that includes renewed state competition with Russia and dynamic instability fuelled by radicalization and extremism from organizations such as the so called "Islamic State" (IS). At the 2014 North Atlantic Treaty Organization (NATO) Wales Summit, decisions were taken by NATO Allies to undertake the biggest reinforcement of NATO since the Second World War (WW2) to respond to this changed security environment. Much of this reinforcement is embodied in the Readiness Action Plan (RAP) – a NATO plan to ensure that the Alliance is more ready and responsive - which will be delivered at the 2016 Warsaw Summit. As this reinforcement gets closer to completion, Allies are increasingly showing their ability to respond to the changed security environment more effectively and rapidly.

But ambiguity in these threats still is a challenge for NATO on how to respond. Both Russian and IS strategies have elements of hybrid warfare, which goes hand in hand with ambiguity. This inevitably complicates things. RAP gives NATO a military response capability, but ambiguity makes the decision-making process of 28 NATO Allies and their ability to use this capability quite challenging: what one nation may see as a threat is sufficiently opaque as to make another nation think it is not; ambiguity also challenges prioritization of how to respond or at what level to respond; ambiguity is better understood by those who are surrounded by it than by those who are not; when a threat is unclear as to where it originates, this contributes to makinge it very difficult for 28 allied nations to reach consensus on how to proportionally or appropriately respond without escalating tensions. Responsiveness is just as much about making quick decisions as building military capability. A quick decision to act can be a good deterrent but, if the threat is ambigu-

Ms. Heidi Meyer, NATO Allied LAND COMMAND, Izmir

Heidi Meyer is Political Advisor to LTG John Nicholson US Army, Commander NATO Allied LAND Allied LAND COMMAND in Izmir, Turkey. She came to Izmir from the US Department of State (DoS), Foreign Service Institute in Virginia, US, where she was the faculty coordinator for the Civilian Security, Conflict Response and Prevention program. From 2009 to 2011, she worked at the US Embassy in Kabul as US Department of State lead for Sub-National Governance and Stabilization. In 2009 she worked at the US Department of Defence (DoD) as the Office of the Secretary of Defense (OSD) Policy representative of the Ambassador Holbrooke US Afghan Presidential Election monitoring team. She was Country Director of the US Afghan policy desk in the OSD, Under Secretary for Policy from 2007 and 2009 under the Bush and Obama administrations. From 2006 to 2007 she worked for the US DoD in the Afghan Presidential Palace helping to build capacity with new officials in the Afghan National Security Council and on police reform. From 2003 to 2006 she was Deputy Director of Operations at US Army NATO, SHAPE in Belgium. From 1999 to 2000 she worked for NATO as a civil-military affairs NATO staff officer at NATO Headquarters Naples, Italy and as civilian CIMIC desk officer during the Kosovo crisis. In addition to positions in NATO, US DoS and US DoD, she has been a High School teacher in Italy; founder and Director of the Joint Relief International NGO delivering humanitarian aid to forty countries; British Army Officer serving in Germany, London and Cyprus; Associate Director of Admissions at Dartmouth College New Hampshire, US, a journalist and a ski instructor.

ous, some nations worry that the decisions to act will escalate or exacerbate the situation. So, by taking this into account, NATO will continue adapting beyond RAP to be able to better deal with ambiguity and to be better able to gauge how to respond in order to deter an ambiguous threat. Building consensus about an ambiguous threat and agreeing on how to respond in a consensus-based organization such as NATO is difficult - but it is not impossible and there are definitely areas where NATO can and will improve to be able to respond to ambiguity.

This article discusses some measures that NATO could consider taking up to adapt to ambiguous threats so that decision-making is not so challenging and political and military responses are at the right level and at the right time with more options. These measures are: Support to building Allies and Partners national resiliencies as a first line of defense; improving intelligence sharing and analysis for early indications; building a wider security network with civilian and military partners; developing a more substantive NATO cyber defensive capability; putting Strategic Communication (STRATCOM) at the heart of NATO response and developing strategies for responding to propaganda; reviewing NATO nuclear deterrence policy; and using these measures by calibrating a response to ambiguous threats through a carefully designed comprehensive approach of political, non-military and military responses.

Before examining each of these measures in more detail, it is worth reminding of NATO's central plan to be more ready and responsive. This plan is RAP, which is the basic platform from which NATO will respond to ambiguous threats as well as to conventional threats. RAP includes the Enhanced NATO Response Force (NRF) with its spearhead the Very High Readiness Joint Task Force (VJTF). These newly adapted military response capabilities will enable NATO to respond to conventional threats and to deter ambiguity. However, in deterring ambiguous threats, it is expected that NATO will want to do more. Along with RAP adaptation, NATO also has to ensure that it has a holistic approach to responding to ambiguity. Therefore, NATO will need to further adapt to ensure a political, institutional and military comprehensive approach, which is far more effective in dealing with ambiguity than simply a military response alone. The following sections discuss how and where NATO needs to further adapt to deal with ambiguity.

BUILDING ALLIES AND PARTNERS NATIONAL RESILIENCIES

The Russian way of making war is to avoid confrontation – why use military means if you can achieve your objectives by non-military ones? The Russian strategy is to use all elements of national power including political, military, economic, and propaganda and information operations below the military confrontational threshold. The Russian Gerasimov Doctrine tells us that Russia will likely fight undeclared wars through a strategy that is constituted of four non-military parts and a military one. The aim is achieving Russian strategic objectives without overt confrontation. A major element of the non-military part of the Russian strategy as laid out in the Doctrine is made up of propaganda, misinformation, psychological manipulation, and use of social media. However, there are other aspects of the plan that include undermining governance, subverting a nation's economy, fomenting dissent amongst Russian speaking peoples and generally overtime disrupting stability through non-military means. These tactics are ambiguous by nature – and designed to be that way.

The first line of defense to combat these non-military and ambiguous tactics is organically by the targeted nation. Nations are in the best position to understand when Russia is undermining their national stability and to instigate effective counter measures early on. However, national resilience to Russian non-military hybrid measures is better when supported by international organizations such as the European Union (EU) and NATO. The EU can help funnel the right level of economic support and opportunity to help a country in its effort to build resilience. (Countries with economic challenges are almost always more vulner-

able to outside manipulation and aggression). NATO can show support and solidarity with an Ally who counters hybrid aggression through assurance measures, exercises, joint training, presence and NATO high level visits. NATO can also help nations develop Advanced Plans in order to make them ready to militarily respond to an aggressor – with a built in element of the plan being NATO support. This demonstration of support must last in the long term as long as the aggression continues. One of the ways to continue supporting is through good intelligence and information sharing as it informs about the shape, size and feel of that aggression – and how ambiguous it is.

Without early indicators and warning there is no trigger to tell us an ambiguous attack is underway.

BUILDING A STRONG INTELLIGENCE SHARING NETWORK

Over time, good intelligence is critical to tracking and overcoming ambiguous hybrid warfare strategies waged by an adversary. Building the history, the picture, and the patterns of a hybrid strategy used by an adversary helps overcome ambiguity. Hybrid strategies tend to create a "new normal" whereby we become inured to the effects overtime of a hybrid warfare strategy and thereby contribute to the intent of our adversary to make their strategy ambiguous. The adage of putting a frog in cold water and slowly building the heat over time so that the frog doesn't notice is the best way to describe this. Good early intelligence that builds a picture overtime will tell us about rising water temperatures and when it is reaching the boiling point – and indeed if the frog is about to boil! But the special challenge with ambiguity is that, intelligence must be gathered from civilian sources as well as from military ones because of the non-military component of this type of warfare. Arguably, the civilian or non-military intelligence sources are more important to build a long term well informed picture. For example, an experienced economist of a country knows best when the economic prosperity and well-being of his nation is being compromised by underhand actions; a government official knows when the governance structures of his country are being slowly eroded; a policeman knows when the rule of law is compromised or the criminal elements of a country are organized and complicit in a hybrid strategy of aggression; and an activist in the civil society has an opinion when the country's values and democratic institutions are under threat. So, we must use academics and practitioners who normally do not contribute to military intelligence. We must use social media and open sources and collaborate with civilian organizations. Sometimes, we must tap into unorthodox sources. NATO's writ does recognize the importance of being able to cast a wider net amongst civilian communities in intelligence gathering and to build an analysis capability that can fuse a far wider range of civilian and military data. So now we must do it and nations must support us. Traditional sources of military intelligence gathering are no longer enough. We cannot complacently reach "new normals" and accept or ignore these new levels of ambiguous attack or worse still reach the new normal without realizing it – we must have strong intelligence that builds a substantive picture over time (sometimes over a long time) and that explicitly warns us when hybrid strategies are reaching new thresholds and allows to attribute our intelligence by showing a build up of patterns over time. This will take out a lot of the ambiguity in hybrid warfare and will allow coalitions to more quickly make important decisions when they need to about responding to hybrid warfare attacks. In widening its intelligence network, NATO should certainly benefit from the open source knowledge of its Partners.

A SECURITY NETWORK OF PARTNERS

NATO recognizes the role that our Partners play in developing a security network that offers much in terms of military capability. The additional value of Partners is their local and regional knowledge and the contribution they make, not just to better the understanding of regional geo-strategic politics but also of real life activities on the ground. Their view is important and counts for much. In the current environment and beyond the NATO Summit to be held in Warsaw in 2016 much emphasis is and

will be placed by NATO on the role that Partners can play in helping to bring additional capabilities in strategies to counter ambiguous threats – including their regional knowledge.

The very fact that NATO is an Alliance of twenty-eight nations but that can extend out to many more nations in a security partnership network is of great deterrence value. This value is in terms of building a picture of threat and local knowledge. NATO can now develop the mechanisms to wisely use that knowledge.

STRATCOM AS THE CENTRAL ELEMENT OF OPERATIONAL PLANNING

Russia annexed Crimea by using clever propaganda or, as the West says, a clever strategic communications strategy (SRATCOM). Both Russians and IS use propaganda as a weapon of war. Modern hybrid warfare is arguably made of the old ways of waging war but with more intensity in the use of information and modern technology to spread a message. This is exploited as a deliberate deception or propaganda in order to change people's view of the world. Russia was able to boldly invade and annex Crimea almost entirely through propaganda, affecting people's opinions through information and strategic messaging - without firing a shot. Using information as a key weapon in a war strategy is difficult to attribute. This strategy of ambiguity is widely used by Russia. Arguably it is what they are best at. Keeping a strategy below NATO Article V threshold through primarily non-military means offers Russia far greater options over time to achieve its strategic goals. Propaganda and use of social media is a central element of this approach and the most difficult ambiguous threat to attribute and respond to. Putting aside Russia TV, which is widely used, and fairly obviously Russian propaganda, the most difficult propaganda to respond to is the widespread and informal use of social media. How does a nation respond when it is under an attack from propaganda that is deliberately misleading or wrong and designed to misinform and change people's opinion of events and motives? Ukrainian organization StopFake.com is a good example of an organic response by civil society to directly refute or debunk stories on social media. This type of grass roots response to propaganda is based on volunteerism and open source information and could be replicated in other countries where propaganda is being used. We should also pay attention to civilian scholars and practitioners who are developing thought in this area and especially encourage and reward young innovative thinkers. For instance, one of the most forward leaning young thinkers in this area is Ivana Smolenova who delved deeply into the Russian use of propaganda. Her work is just beginning and with support she will develop a body of understanding and expertise that we sorely need into the future. There are also think tanks working in this area. One example is Legatum Institute's series Beyond Propaganda. This was designed to help us all be better equipped against "media manipulation across the world, and will inform the work of policy-makers looking for innovative ways to win the 'information war'." Also, a notable thinker associated with this subject is Peter Pomerantsev, who is Senior Fellow to the Legatum Institute's Transitions Forum. His book "Nothing is True; Everything is Possible" is widely regarded by many in the hybrid warfare business as fascinating revelations about misinformation. Military Institutions do not naturally develop quick thinking in the realm of propaganda – it is not what they train for and it is not in their DNA. But if an adversary uses propaganda as a central element of its war strategy, the Western military and defense institutions will need to adapt to respond. They will need to reach out to innovative civilian thinkers such as the ones mentioned above and embrace their work. The military may also have to seriously consider putting STRATCOM as a central element of their operational art of war rather than as an "also ran" or distant second to military planning in fire power and maneuver.

BUILDING CYBER DEFENSE CAPABILITY

Hybrid warfare is as old as the Trojan Horse with some new twists. One of those twists is in the cyber domain and in the increasing threat of ambiguous cyber attacks. NATO must continue developing its Cyber defense policy and capabilities so that a cyber attack can be quickly attributed. This is a challenge

in an Alliance of 28 nations all with different national cyber policies and practices. It also requires close cooperation with the corporate world - something the military doesn't naturally do. In the cyber domain, where the chances of an ambiguous threat are ever present, all of these challenges will have to be overcome to enable NATO to make quick attribution of cyber attacks and thus quick political decisions on how to respond.

REVIEWING NUCLEAR DETERRENCE CAPABILITY

In 1967, under U.S. leadership, the Alliance formulated the doctrine of "flexible response". According to this doctrine, NATO would use whatever means necessary to deter or repel a Soviet attack. Conventional forces would be initially engaged, but the United States pledged that it would use its strategic nuclear arsenal if conventional forces failed in the defense of western Europe. Use of nuclear weapons is not ambiguous but the threat of using them is - and over the past two years Russia has made- hints and even brazen threats about their willingness to use nuclear weapons early in the fight. If NATO had an updated nuclear deterrence policy, this might go some way to deterring ambiguous attacks including the strategic messaging plan that goes along with it. But will the same idea of "flexible response" work this time around? Can we achieve the same levels of deterrence with conventional weapons? And how do we know if the Russians are using propaganda once more to fragment and confuse the decision-making process in the West rather than seriously making threats? The key is to review our nuclear deterrence policy soon and ensure that it is agreed and able to respond to the Russian new nuclear policy. And then we must train and exercise that response.

CONCLUSION

The approach to ambiguity and to overcoming ambiguity must be a calibrated comprehensive approach to thwarting ambiguity. This should include all the above tools working together in a carefully calibrated, consistent design to deter through swift strong military response, debunk propaganda, attribute threats and build local resiliencies. Military strength alone will not work. Fragmentation and inconsistency will not work either. Lack of strategic patience will not help at all. NATO and the West tend to get impatient with the notion of strategic patience. Their ability to pull together a variety of measures in unity of effort consistently overtime is subject to all sorts of influences including national politics that debunk the intent. If we want to overcome ambiguity, we will have to become very adept and clever at using military and non-military strengths in an overtime consistent integrated design that has a core immunity to influences. The greatest strength that the Alliance has is unity and comprehensive action with the "28" as well as with Partners and civilian organizations such as the EU. However, NATO must use it constructively and comprehensively. According to Peter Pomerantsev, "the 21st century will be remembered as the century of the "contactless" war, where perception is everything and maskirovka—military strategy of deception—rules." (Legatum Institute, 2015) This means that there are two important strengths to develop as we move into the 21st century, namely military strength, and flexibility and responsiveness that credibly deters ambiguous threats and the ability to overlay thematic military deterrence with a very strong capability of partnering with non-military capabilities. The challenge for military Land Forces is that they naturally are very good at the military response part of this but not at linking it with the non-military part. So, they have to branch out and be creative and unorthodox in developing compatibility with the non-military elements of a counter ambiguous warfare plan. Will they do it? All the indications are that they will eventually do it but it will take patience, understanding and an open mind. Many of the recommendations in overcoming ambiguity are about mind shifts and breaking paradigms not about the actual mechanics. A mind shift to move beyond conventional military responses into an area of non-military partnerships, strategic messaging, resilience building, non-military intelligence gathering – areas soldiers are not so comfortable in, - more than anything will be our greatest challenge in overcoming ambiguity.

Hybrid threats on energy infrastructures and supply lines

Mr. Christophe-Alexandre Paillard, Strategic Research Institute of the Military School, France

**The views expressed here are solely those of the author.
They do not necessarily reflect the views of the IRSEM or any other organization.**

Today, European countries, more specifically the members of the European Union (EU) and the European members of the North Atlantic Treaty Organization (NATO), are being confronted to five key energy challenges. Firstly, emerging countries are more and more taking a major part in the world energy balance, limiting developed countries' market power (such as the one of the United States), to impact world energy prices.

Today, European countries, more specifically the members of the European Union (EU) and the European members of the North Atlantic Treaty Organization (NATO), are being confronted to five key energy challenges. Firstly, emerging countries are more and more taking a major part in the world energy balance, limiting developed countries' market power (such as the one of the United States), to impact world energy prices.

Secondly, among the EU and NATO member states, more and more countries, such as Germany, Italy and Belgium, are giving up their nuclear industries, because of the strong position of anti-nuclear public opinions, leaving the path to hydrocarbon forms of energy such as coal, oil and gas. Therefore, the end of many European nuclear industries will mean more external energy dependencies for an increasing number of European countries. It will also increase the number of possible hybrid threats on long distance energy supply lines and on key producing areas such as the Middle East or Russia where most of the energy imports come from. Thirdly, European countries should think twice when closing some of their key energy infrastructures because many energy producers are located in instable areas, although the recent development of shale gas in Northern America, of offshore oil in Brazil, and of offshore gas in

Mr. Christophe-Alexandre Paillard, Strategic Research Institute of the Military School, Paris

Christophe-Alexandre Paillard is Research Director in charge of armaments and defence economics at the Strategic Research Institute of the Military School, (IRSEM)[1], French Ministry of Defence. Previously, he was Deputy Director at the Strategic Affairs Directorate (DAS) of the French Ministry of Defence; Head of the international, technological and legal departments at the French data-protection independent authority (CNIL); Senior Adviser in the cabinet's office of the European Affairs State Secretary (SEAE) of the French Ministry for Foreign Affairs. For several years, he has specifically worked on topics such as energy supplies, strategic and critical minerals, key defence technologies, industrial and economic risks that could have consequences for national, European, and North-Atlantic security. He has developed specific competencies on Latin American and Spanish economies. He is a senior lecturer in economics. He is the author of books and articles on oil, minerals, smart grids, gas supplies, coal industries or defence issues.

[1] Strategic Research Institute of the Military School, (IRSEM) is a French research centre with the status of national service attached to the General Directorate for Strategic and International Relations, French Military of Defence (DGRIS). Its goal is to support and to promote research in the area of defence and security. Its production is focused on international defence and security. It is openly accessible worldwide. Publications cover Armament and Defence economics, Defence studies, Strategic studies, and Defence and Society. It provides academic and financial support to young researchers, following doctoral and post-doctoral studies. It is responsible for steering and facilitating the approach to forecasting and strategic research. Refer to: http//:www.defense.gouv.fr/irsem

Australia has reshuffled the cards to the disadvantage of Russia, of the Middle-East and of North Africa areas on world energy markets. It is worth noting that nuclear power plants could help us to limit terrorist risks as well as unconventional attacks outside Europe. Fourthly, all European countries, including France, Britain, the Baltic States, and Spain will be confronted with a triple challenge: energy security of supplies, economic efficiency and environmental needs. Finally, the last challenge European countries will be facing is their ability to settle a common approach to their energy security key issues, to the consequences of climate changes on their security, and to common possible threats, including hybrid ones, on their key energy infrastructures in a close future. Unfortunately, looking at the political, social, economic, and strategic difficulties that Europe is now facing, a common approach to all these topics in the next years seems very unlikely. Thus, a comprehensive approach to energy issues, including the possibility of confronting a rising number of hybrid threats (which do not concern only economic and industrial issues), is essential to understand the current challenges we all face. Clearly, European countries need to understand and anticipate possible risks and new possible threats on energy infrastructures and local economies, because we will face a growing vulnerability of our energy infrastructures in case of unconventional conflicts. This is one of our main challenges.

TYPOLOGY AND ORIGIN OF POSSIBLE THREATS ON ENERGY INFRASTRUCTURES

NATO and EU member states need to define a typology of targets and priorities in terms of security. When terrorism is concerned, various targets are highly vulnerable. They include permanent military infrastructures (e.g. headquarters, ammunitions dumps, fuel depots, spare parts storage, barracks, etc.), high valued mobile military aircrafts (e.g. Airborne Warning and Control System planes, supply planes, carriers, fighters, bombers, etc.), radars, aircraft carriers, as well as logistics and chains of supplies (e.g. means of conveying, landing and boarding: ships, cranes, docks, bridges, roads, control towers, runways, etc.; and other suppliers such as generators, power lines, tankers, gas tankers, nuclear facilities, etc.). Finally, targets can also be political, such as decision centres (ministries, key administrations), hospitals, civilian power plants such as nuclear power plants in countries such as France or the United States, and highly populated areas.

Figure 1. Petroleum depot, Gao, Mali (July 2015), French Joint Petroleum Service (SEA), Ministry of Defence of France

The Middle East and Northern Africa (MENA) is the world area where it is key to anticipate threats on energy infrastructures, which mainly include industrial and business targets such as production sites, factories, civilian gas or oil depots, goods stations, and oil and gas companies. In a way, the 9/11 attack in New York was a turning point: before 9/11, Western policy objectives included dual containment (Iran/Iraq), preserving access to oil and gas, and promoting democracy. After 9/11, policies shifted on changes in security and on promoting pre-emptive action ("real and imminent threat") and regime change. This did not stop terrorism, extreme Islamism and instability in the MENA area at all: the contrary just happened. As MENA is dominated by wars and instability, it is tricky to define what a terrorist threat could be. Basically, the purpose of terrorists is to send a political message to the Western world and to induce fear in people. There was a time when they were massively state-sponsored, especially during the Cold War, but that time is over. Now, terrorists are much more like Al-Qaeda or ISIS. Many are fighting against any form of Western influence in their homeland, like in Syria and Iraq. We must then wonder what the strategy of these "terrorist organizations" could be. Basically, they all try to pressure Western influence on energy out of their countries through terrorist attacks. If Al-Qaeda were first founded to overthrow the Saudi Arabian government, it would get a much broader scale agenda on the long term, like other terrorist groups such as ISIS, leaving us with higher difficulties to retaliate when needed.

Launching an attack on energy infrastructures, as for example in the case of Iraq, leads to immediate prospects of death and destruction. In this case, energy systems are clearly war targets for many, such as ISIS or other political movements fighting on the ground. To cause huge damages, terrorists need economic and social disruption, the creation of ripple and synergistic effects, the destruction of critical nodes impacting transportation (pipelines, port facilities), and the production of bottlenecks such as oil refineries. In other areas at war, such as Mali and the Sahara desert, there is also instability, but energy targets are limited. France went to war in Mali to avoid regional instability in Western Africa and the potential disruption of an Islamic state in Sahel. In the long term, such a state might also have led to potential energy disruptions in Western Africa and in the Sahara desert and to serious damages to oil infrastructures or uranium mines in Niger. The attacks on the Algerian Sonatrach and gas facilities from Islamic leader Mokhtar Belmokhtar and his MUJAO movement in In Amenas and in the Algerian Sahara desert in January 2013 showed what could have happened in many other places close to combats' areas if France had not blocked local extremist movements such as AQIM (al-Qāʿidah fī bilād al-Maġrib al-islāmī), Ansar Dine and MUJAO. In the case of In Amenas, a hostage crisis started when some Al-Qaeda-linked terrorists, affiliated with a brigade led by Islamist leader Mokhtar Belmokhtar, took expat hostages at the Tigantourine gas facility near In Amenas. One of Belmokhtar's senior lieutenants, Abdul al Nigeri, led the attack. He was among the terrorists killed. After four days, the Algerian Special Forces raided the site in an effort to free the hostages. 39 foreign hostages were killed along with an Algerian security guard, as were 29 terrorists. This operation allowed a total of 685 Algerian workers and foreigners to be freed.

TARGETING OIL AND GAS PIPELINE TERMINALS IS A NATURAL STRATEGY, BUT DOES IT WORK?

Pipeline terminals are possible targets for terrorists. However, key terminals such as Ras Tanura in Saudi Arabia are well protected. Everyday 7 mb/d leave Ras Tanura, in the north of Bahrain, making it an enviable target for any coordinated action, terrorist apprentices and potential kamikazes. Neutralization of oil exports, even limited, is by nature able to disrupt world oil and gas markets and to increase oil futures on a still unknown scale. Even a simple try would have side effects on traders and financial actors for a few days before returning to a cooler behaviour.

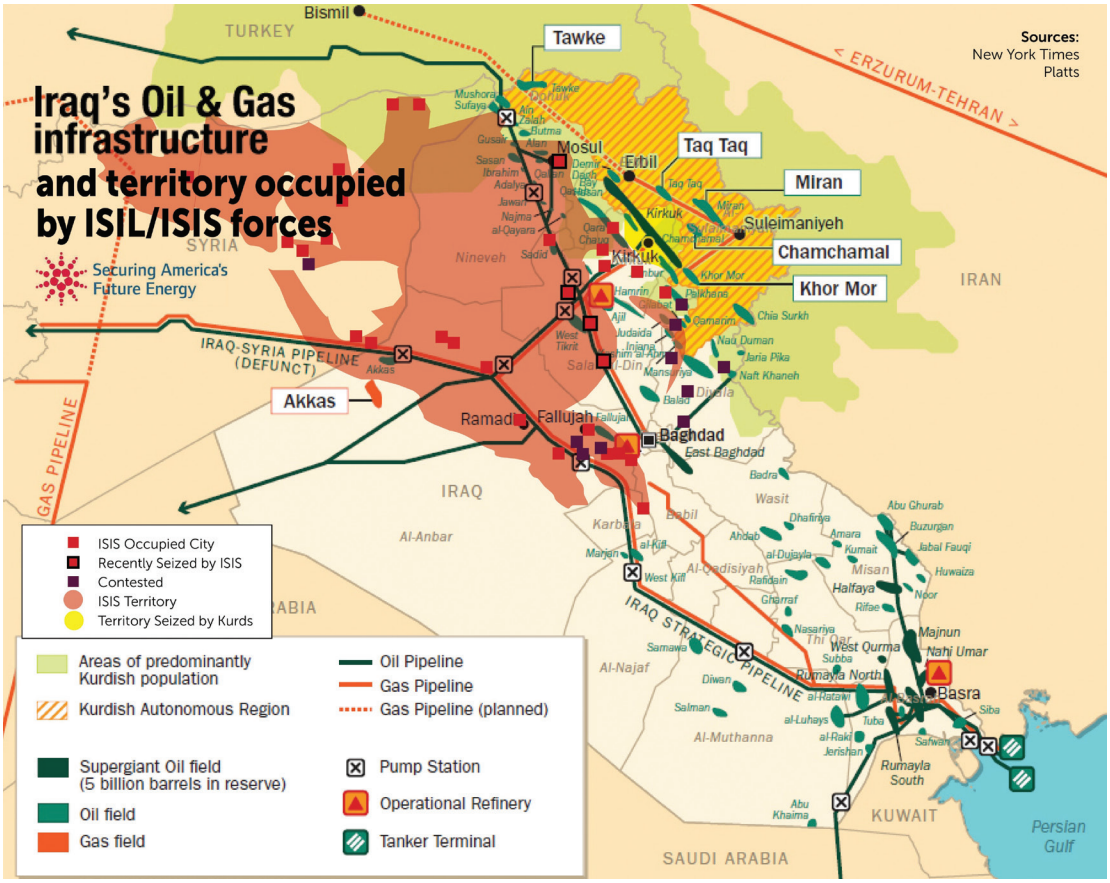

Figure 2. Iraq's Oil and Gas infrastructure and territory occupued by ISIL/ISIS forces

The real nightmare would be a "blockade" of the Strait of Ormuz, connecting the Gulf of Oman and the Persian Gulf. It would be successful even if the blockade were not a physical one, but something impossible to achieve by terrorist means, that is to say a form of invisible barrier, which would prevent ships from coming into the Arabian Gulf without any substantial new insurance policy. In order to succeed in organizing such an operation, a complete network of supporters, well-equipped teams, and a bit of intelligence from terrorist organizations would be necessary. However, in this last example, we are in fact leaving conventional terrorism and we are back to conventional war and state support of violence against energy infrastructures, which is a completely different subject.

It is difficult to find a way between an underestimation and an overestimation of threats on energy infrastructures. This is because the right analysis is the most difficult target to reach. Should we expect a new wave of terrorism on energy supply routes? Is the main threat on sea routes? In this context, it is worth considering that various forms of terrorist risks could potentially threaten the European economies and the traditional energy routes, both at sea and on the ground, which can be used for oil and gas. The notoriously most threatened areas in the European southern neighbourhood are the Arabian Gulf, the surroundings of Yemen and Somalia, and the Suez Canal, which are potential terrorist targets. Shipbrokers and ship-owners, such as Clarksons or many others registered on the Lloyd's list[2], awakened to the tough realities of terrorism when the Limburg was blown up in Yemen in 2001. But, apart from this noticeable attack on a tanker at sea, nothing really happened since then and the Limburg is still

[2] See: http://www.lloydslist.com/ll/news/top100/brokers/

considered as an exception by experts when threats at sea are being evaluated. Precautionary measures to increase the number of ships and to speed up crude oil movements have often been useless. It does not mean that what happened to the Limburg could not happen again; but it is quite unlikely today.

Though the impact of the Limburg bombing was close to zero on the long term, European states cannot underestimate the feasibility of broader attacks and should give a specific watchfulness on their energy supply routes over the next years. Due to the position of the European states towards the Islamic State and other Islamic movements, new terrorist attacks on pipelines, tankers, and liquefied gas carriers could disrupt European economic stability and security.

Maritime routes are certainly at risk, but this risk cannot be overvalued, due to the limited number of forces that the European countries can deploy around the Indian Ocean. Over the last years, French naval forces were thus frequently left alone by other European countries to play the police force at sea, if one leaves apart the Atalanta operation. In fact, the Atalanta operation, also known as the European Union Naval Force Somalia (EU-NAVFOR-ATALANTA), was a counter-piracy military operation at sea, off the Horn of Africa and in the Western Indian Ocean. It was the first operation undertaken by a European Union Naval Force. This mission was launched in December 2008, with a focus on protecting Somalia-bound vessels and shipments. Atalanta also monitors fishing activity on the regional seaboard. In 2012, the scope of the mission expanded to include Somali coastal territories and internal waters, aiming at coordinating counter-piracy operations with Somalia's Transitional Federal Government and regional administrations. On the 16th July 2012, the European Union mandated the European Union's capacity building effort in the Horn of Africa and the Western Indian Ocean (EUCAP) Nestor mission to build up the maritime capacity of regional navies. Additionally, Atalanta is part of a larger global action of the EU to prevent and combat acts of

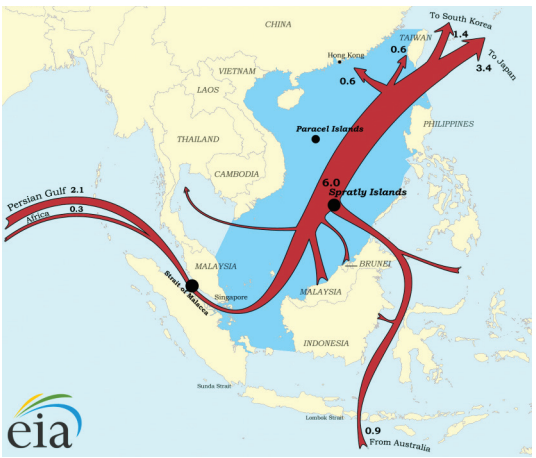

Figure 3. Major reade flows in the South China LNG Sea (2011)

piracy in the Indian Ocean, which is combined with the US-led Combined Maritime Forces (CMF) and NATO's anti-terrorism Operation Ocean Shield.

Therefore, maritime routes used by tankers are under pressure. However, this pressure should be better valued: a feeling of insecurity and anxiety developed among Western forces, oil and insurance companies after 2001. They thought that there were some high risks of possible disturbances at sea on oil and gas supply routes. However, for a while, they did not really take into account that only one single ship had been attacked in 14 years, which was the Limburg. The threat was thus a little bit overvalued. In the eventuality of a large-scale political crisis of any kind around the MENA area, the strategic landscape might be different and terrorism at sea could be much more scrutinized by Western chiefs of staff and European states in case of war in this area. Risks on maritime transports should be considered together with many other threats. It is necessary to take into consideration many forms of risks such as piracy, broad safety on maritime routes, geopolitics of straits, balance between various means of transports, and the true nature of physical risks on oil and gas maritime routes.

As shown by the Limburg case, if there is a risk on oil and gas maritime routes, damages would not be huge enough to destabilize oil

markets: the feasibility of inflicting significant damages on a ship depends on geographical, technical and physical conditions which are scarcely met. Although the destruction of a few ships should certainly increase insurance's prizes, it wouldn't certainly disorganize the world maritime traffic on a period long enough to have durable impacts on world energy markets. Only a much more global war could do this and there are clearly a few oil transit chokepoints to target.

SINKING SHIPS IS A VERY HARD BUSINESS IN ITSELF!

Weapons or explosives have various effects, depending on the angle, the strength of the explosive charge, the rate of fire, the track course or the point of impact. A simple RPG7 rocket-launcher is able to damage and to make a hole in the hull of any ship and in double-bottom tankers. However, this does not mean that the targeted tankers would go off easily. Against this kind of weapon, which is easy to get on markets, there is no protection efficient enough to protect all commercial ships sailing at sea. If a military escort could be provided during wartime, it would not seem realistic enough for Western navies to do it also in peacetime or to equip commercial ships with heavy military capabilities.

The explosive capacity of ships, far beyond the strength of the explosive charge, is also a key element to succeed in sinking them. Whether a ship is full or empty, it has little chance to explode. When the ship is full, the fuel gets a capacity to absorb chocks, which makes the feasibility of having an explosion unlikely. For instance, when the French clandestine Organisation de l'Armée secrète (OAS) launched an attack on gasoline depots in the Antibes (in southern France) in 1962, it failed because the tanks were full and had limited explosive capacities. By contrast, if a tanker is half empty, the gas in suspension in the empty part of the ship makes an explosion more likely, even if it is present in very limited quantities. Although this risk of explosion is limited, there is indeed a bad combination of a highly inflammable mix of oxygen and hydrocarbons, which could provoke an explosion in case of a sabotage aimed to damage a harbour or any key infrastructure.

States have different approaches to these matters. For energy consuming states, the risk is limited to the possibility of being confronted with temporary cuts of supplies. When the Suez canal was closed in 1956 or when the Iran/Iraq war partly blocked ships in the Arabian Gulf, Western countries feared that their economies could be damaged by a long-term blockade. This kind of risk partly explains why the American policy in the Middle East aimed at showing military strength in the area and at deploying noticeable naval forces, like in the case of Kuwait in 1990. However, terrorism has not been responsible for any significant blockade in the Middle East over the last 70 years. For energy producing states, the risk is far beyond the risks that consuming states could be confronted with. The former could suffer from complete exports' blockades. If producers are confronted with temporary impossibility of exporting oil and gas for physical or psychological reasons, what is at stake is the sake of their whole economies. However, again, no terrorist act has been responsible of large blockades, even in the MENA area.

A POSSIBLE SCENARIO OF UNCONVENTIONAL ATTACKS ON EUROPEAN ENERGY INFRASTRUCTURES: NEW GRIDS, NEW THREATS?

Leaving apart the MENA area, sea routes, and traditional targets, hybrid threats on energy infrastructures are emerging, such as those on the electricity system. Europe is building new grids, because it needs a more efficient electricity system as well as new distribution networks to face the growing complexity of systems management and a possible growing gap between energy supplies and demand. New European grids mean stronger interconnections within the European electricity system. The existing interconnections could go beyond their present limits extending to the South, across the Mediterranean Sea, and possibly reaching the Russian electricity system. The recent opening of electric-

ity markets led to the development of smart meters such as Linky in France in March 2009, which is the cornerstone of smart grids in a new European distribution network. The European Commission targets 80% of smart meters in the European Union in 2020. Networks are indeed moving from a passive to an active position through the development of decentralized power generation. Smart grids might therefore be potential targets for unconventional attacks.

Smart meters should start covering the whole France in 2018. France is preparing to embrace "smart meter" technology on a massive scale. Indeed, 90% of French smart meters should be replaced by 2021, as imposed by the 17th August 2015 French law. "Smart meters" or "communicating meters" are electronic boxes, which replace traditional meters on a building's switchboard. Their distinguishing feature is that they connects directly, mainly via Internet, to the grid management system. Thus, this new generation of meters provides all power managers, distributors and customers with instant access to information on real-time power consumption. These data should enable power suppliers and distribution service operators such as Electricité de France (EDF), Direct Energie, Poweo, Gaz de France/Suez now called ENGIE, and others to finely tune power used by consumers over the short, medium and long term. In France, Linky meters are supposed to replace the old EDF meters across the country. Linky will communicate data remotely, transmitting directly to Electricité Réseau Distribution de France (ERDF)'s supervision centre.

How smart meters and smart grids are going to work is a key point that must be understood. Smart meters intend to measure and control home electrical consumption precisely. However, this could erode the privacy of daily life, unless regulators limit data collection and disclosure, and maybe even national security. Indeed, in the absence of clear rules, these potentially beneficial smart grid technologies could mean intrusion into security, leaving apart privacy. Utilities collecting detailed information about energy use at home must specify in advance how they are going to use data and must confine their collection to legitimate purposes. Furthermore, utility companies should ensure that consumers have access to their own data, so that they can take advantage of innovative energy efficiency services, and explain clearly where data are stored and how they are protected. The load graphs gathered by advanced energy metering projects allow the reconstruction of everyone's life: when you wake up, when you get home, when you go on vacation, and so on. These are clearly potential targets for terrorist or criminal organizations.

Protecting European citizens from hybrid threats on smart grids is thus a necessity. Smart grids intelligent monitoring devices are in fact vulnerable to criminals and terrorists. They might be the next main cyber security threats on smart networks in Europe. These smart grids and smart metres are vital information pertaining to the lives of citizens. Cyber attacks can make them vulnerable. As an example, hackers can share the information they get from smart grids or smart metres with external hostile political or criminal movements. In fact, the usage of data stored in the utility server could be stolen and misused. In order to preserve security, energy companies should use anonymous data packets containing the usage information, but not the user's information. This approach allows the utility companies to forecast load in a region, but not to enable the utility companies to keep individual usage data to advice the consumers regarding their energy usage habits. Security is not only a way of keeping energy markets safe and reliable in Europe, but also a global process,.

***

More attention to the security of energy infrastructures will be required in the next years. Controlling maritime routes is in fact a key element for successful strategies against any potential terrorist activities. Since World War II, the link between freedom at sea and oil supplies has been strong, noticeably enough in western powers' foreign policies. But terrorism is not a

global threat on maritime routes. Gas and oil pipelines are more local and regional when compared to maritime routes. They are largely on the ground and only sometimes under the sea, like in the case of the North Stream. Thus, some pipelines could be major strategic targets, like in Ukraine. However, although bombings have been frequent in Iraq in the last 12 years, they have not changed the world energy balances. They have only impacted the local forces and the populations directly involved in the area of the bombings.

In conclusion, growing political instability in the MENA area is a key constraint to the international strategic configuration. Although the move towards a multipolar world is not yet complete, the changes occurred in the international system are raising a number of questions: how do we define our defence policy? What impact does the economic crisis have on conflicts and on our military capacities? Is energy the next battlefield for Islamist movements? Is Ukraine the next step towards energy insecurity in Europe?

The energy weapon that could not
Assessing the European energy security in the stand-off with Russia, 2014-2015

Mr. Václav Bartuška, New York University, Czech Republic

Motto:
"Global economy will collapse if oil prices remain at $80 per barrel."[1]
Vladimir Putin, October 17, 2014

Over the last two decades, many worried that should Russia decide to confront the West once again, energy could become its most influential weapon. Being the world's largest gas producer and the second biggest oil one, the argument was that Russia had huge leverage. Europe would freeze without Russian gas, while the lack of Russian oil could bring the global economy to standstill, wiping out the Western economic dominance. In other words: be nice to Russia, otherwise...

We have the opportunity to test this theory in real time. Let us have a look at the results so far.

NO GUNS

This article focuses on the softer part of West's power, meaning its influence on glob-

Václav Bartuška

Václav Bartuška has worked as Ambassador-at-Large for Energy Security in the Czech Republic since 2006. Over the last decade, he has been involved in many energy issues. In January 2009, he was a point-man of the Czech EU Presidency during the Russian-Ukrainian gas crisis. Afterwords, he worked for the Swedish EU Presidency on the same issue. Mr. Bartuška was one of the student leaders in the Czechoslovak "Velvet Revolution" of 1989. He was subsequently appointed by the Parliament to investigate the former Communist secret police. He currently teaches at the New York University, Prague campus (since 2003).

[1] "Путин: мировая экономика рухнет при сохранении цены на нефть $80." Meeting with journalists on October 17, 2014, in Milano, Italy. See also the official Russian sources, such as the news agency RIA Novosti: http://ria.ru/economy/20141017/1028841776.html. For the English version, refer to: "Putin: Global Economy Will Collapse if Oil Prices Remain at $80 per Barrel", available at http://sputniknews.com/world/20141017/194226195/Putin-Global-Economy-Will-Collapse-if-Oil-Prices-Remain-at-80.html.

al markets and in particular the strength of the European Union (EU) as a demanding (and also punishing) partner for Russia. For a long time, it has been clear that the EU and the North Atlantic Treaty Organization (NATO) were natural partners. Each of them can achieve goals that the other can not. Few countries in NATO countries want to go to war if they are let alone with Russia. Exploiting EU's economic strength is far easier, logical – and surprisingly effective.

There is, however, a limit to what economic (or any other kind of soft) power can do. It was the fear of a military conflict among the European states that worked as deterrent by keeping the peace in Europe during the Cold War, not the financial strength or clever use of natural resources. We should not fool ourselves into thinking that this time it is different in any way.

FEW DATES TO REMEMBER

Little green men occupied Crimea on 26th-28th February 2014. Well trained and equiped, they missed only one thing: the insignia of their country. Russia denied that they were its soldiers, but few believed that. Crimea was incorporated into the Russian Federation just few weeks later, on 18th March 2014. President Vladimir Putin's speech about *Novorossija* was held on the same day. The *supporters of the federalization of Ukraine*, as they were called by Russian official media, started the war in Eastern Ukraine just some weeks later.

The European Union and the United States (US) responded to this flagrant breaking of the international law by imposing sanctions against the Russian Federation and its helpers in Crimea/Eastern Ukraine. Their effectiveness – and especially the fact that the EU and the US acted in unison – came as a huge shock to the Kremlin. Indeed, it surprised many in the European capitals, as well as in Washington. In particular, the sectoral sanctions, which target the Russian banking system as well as energy businesses, are very severe. Yet it was the economic factor that weakened our opponent the most.

OIL AT 50

For decades, the determinant of the price of oil was the fear factor: an attack on a tanker or a refinery anywhere in the world could cause an increase in oil prices. Global production capacity was low, covering the demand with very little margins. Russia, one of the world's most important producers (together with Saudi Arabia and US), was therefore thought to be in an extremely strong position. Indeed, Russia produces 10 million (mbd) per day of the 90 mbd of oil that the world needs (maximum 93 mbd per day are extracted). Therefore, Russia can clearly wreak havoc should it decide to do so.

This reasoning, however, did not take into consideration the other half of the equation: Russia's extreme dependence on the export of raw materials, in particular oil and gas. Some 60 per cent of the state revenues[2] derive from hydrocarbons. (Russia's resurgence over the last fifteen years is often linked to the oil price going from 10 dollars per barrel in the 1990s to more than 140 dollars per barrel in 2008.[3]) Would any leadership willingly endanger such an all-important source of revenue?

In the end, before Russia could use the oil weapon (if, indeed, it was considering such option at all), someone else did. At least, that is how it looks from Moscow's perspective.

When discussing Western sanctions with Russian counterparts, almost all of them consider the decrease of oil prices as the most damaging factor. You can try to argue

[2] There are many different statistics in Russia. You can find studies claiming that Russian economy is almost 80 per cent dependent on oil and gas, as well as papers stating that less than 50 per cent of GDP is oil-driven. However, nobody disproves the basic fact that Russia depends on the export of raw materials and makes very few high-quality products.

[3] Russians tend to explain almost everything with oil prices. When leading daily newspaper Kommersant recently prepared a special report on the state default of August 1998, it accompanied every event with two numbers: date, and price of oil on that particular day (Мы проснулись в другой стране [We woke up in another country], available at http://www.kommersant.ru/doc/2258104). As if nothing else mattered. It was corruption, inefficient government and waste that led Russia to bankruptcy in 1998, not oil. And to be fair, over the last 15 years, growth has not been due only to oil – if that was the case, Russia would be bankrupt by now.

that the oil price is decided by markets, not by an EU (or NATO) committee. You may even show relevant documents to prove that the oil price is not on the sanctions list. No matter what you do, your partner knows that oil at 50 is part of the devious Western plot to bring the *Motherland* to its knees.

Arguments will be brought forward, historical parallels mentioned. According to the beloved conspiracy theory, the Soviet Union was crippled by the US-Saudi kabal that lowered the price of oil in 1985, defrauding the Union of Soviet Socialist Republics (U.S.S.R.) of the incomes in foreign currency.[4] (You may try to mention other reasons why the Soviet Union collapsed: inefficiencies of the socialist economy, incompetence of the communist leaders, mass murders, etc.; good luck with that.) The fact that oil went from 110 dollars in July 2014 to 50 dollars in December of the same year is seen as a proof in itself.

The fact that *we* do not believe in the existence of forest ogres is not as important as the fact that *our opponent* believes in them.

REAL SANCTIONS, REAL ECONOMY

The sanctions that the West *did* put in place during 2014 are not as easy to explain as the oil price falling. Yet they are potentially far more devastating for Russia. The fact that Russians rarely mention this is stunning: we are threatening their future prospects, yet the only thing they talk about is the *current* price of oil.[5]

Sectoral sanctions limit the access to advanced technologies for oil and gas production. The damage caused by this limitation is clear when you consider a simple fact: Russia, which is one of the leading oil producers, the world's largest gas producer and the owner of vast oil and gas reserves, is not even able to make drilling platforms. Not to mention high quality compressors or good pipes. It lacks the know-how in the most advanced areas, from 3D-imagining to field-management. It is dependent on outsiders as never before.

In the past, Russia managed to open vast oil and gas fields in the most difficult places, such as the Urals, Western Siberia, and the Far North. It did so with scarce resources, huge domestic limitations, and no help. But it was a different country. Until the 1950s it had unlimited supply of slave labour from the concentration camps: Gulag gave birth to many cities, including Vorkuta, Magadan, and Norilsk. The camps were disbanded after Stalin's death, yet living conditions in many settlements were dire all the way till the end of Soviet Union in 1991 and beyond. People accepted hardship on a scale which is difficult to imagine. Only a small part of these daily difficulties was the fact that they had to use instruments and tools made in U.S.S.R., most of which were of inferior quality.

All this has changed after 1991. Why bothering to work on awful drilling platform of Soviet provenience, when you can hire Western service companies to do the job? Why wearing protective gear which protects neither from the rain nor from the cold, when you can buy Gore-tex? If you travelled across different areas of Russia in those years, you would have realized very easily how little the country produced.[6]

This is why sanctions have created problems: there is no easy replacement for Halliburton or Baker-Hughes. Chinese companies, praised as panacea by the Russian press just a year ago, are now rarely mentioned. Replacement of imported goods by domestic production, *импортозамещение*, is still the favorite line in the media, but its results are meagre at best[7]. Factories, which used

[4] One for many: «Механизмы уничтожения СССР и «принцип домино», available at http://www.km.ru/spetsproekty/2011/11/25/publitsistika/mekhanizmy-unichtozheniya-sssr-i-printsip-domino-ch1.

[5] It is remarkable for an industry that needs long-term vision and planning to have long term plans. For instance, companies like Exxon Mobil have 30-year plans. By contrast, Socialist economies had only 5-year plans – and considered themselves visionary.

[6] The butter Anchor from New Zealand, which it was common to find on shops' shelves in Moscow in the 1990s, is something I still can not forget. I can't forget either the fleets of Japanese second-hand cars, which were driven all around the Urals and Siberia and which were absolutely dominant in Russia's Far East, despite the fact that cars with steering wheel on the right are forbidden by law. In Vladivostok even the Police was used to drive them.

to make oil and gas equipment, were either abandoned in the early 1990s or were obliged to shift their production to other areas. Starting to make equipment again will take time – and to make *quality* stuff will take even longer.

It is easy to call on citizens to overcome the „Western blockade". Rhetoric is cheap. Who will posively answer this call is a different question. Moscow has changed a lot over the last 25 years, and so did many Siberian cities – which is impressive since they started from a much lower starting point than Moscow. In particular, the symbol of change are sushi restaurants in Khanty-Mansijsk[8]. Additionally, the real challenge for Kremlin is to persuade people who are used to work with good tools to eat good food and to travel to the sunny parts of the world, to lower their living standards and expectations.

LADA VERSUS FORD, ONCE AGAIN

During the time of perestroika in the late 1980s, there was a philosophical talk about the possibilities among which the Soviet Union could choose in the oil and gas sector. Moscow could either continue to drive Lada, or switch over to Ford. Expressed less poetically, the U.S.S.R. could develop new oil and gas fields with its own equipment (represented here by domestic car maker Lada) just like Tyumen, Urengoy, and Yamburg, or use more advanced tools from the West (e.g. Ford) and hopefully live a better life.

The Soviet Union disappeared, and the new Russia locked its Lada in a shed and switched first over Ford (chosen by some) and then over Ferrari (chosen by few). The metaphysical questions of *perestroika* were answered by real life. Soviet oil fields extracted 8 per cent of the resources from the ground at best. Western companies were able to qucikly improve that rate up to 20 per cent. Personal fortunes of many Russian oligarchs thought that cooperation with the West could be enriching in every respect.

Field management is even more important than drilling techniques: detailed knowledge of geologic structures and pressures underground (thanks to 3D imagining), real-time control of hundreds of physical factors, ability to simultaneously increase pressures across a giant reservoir by pumping water or CO2. Today, command centers of large oil and gas fields have myriads of computers. If you add to this the US know-how of extracting gas from shale and oil from rock formations (*tight oil* technology is getting oil not just from shale, but also from sandstone and lime), you can just see a tail of the Ford.

The Lada-Ford dilemma is back, as painful as in the 1980s. I have no doubt that the Russians can develop oil and gas fields in Eastern Siberia and in the Far North. Kovykta, Chayanda, Talakan field projects and others are no more difficult than the ones of the 1960s and of the 1970s. In Siberia the temperature is still minus 40 Celsius in winter and plus 30 in summer (cold is better, there are no mosquitoes). Distances are as vast as before, permafrost is unforgiving. People are those who have changed, it is not nature.

GIVE US OIL AT 80, OTHERWISE...

Let's come back to the original question – How much has European energy security changed since 2014? I would just say that in the oil sector, our situation has not changed at all. Russia needs incomes. Putin's quote "global economy will collapse if oil prices remain at $80 per barrel" allows us to grasp his way of thinking. He runs a country that is so dependent on the prices of commodities that it has lost track of some fundamental facts. For example, the fact that oil price goes down is a boon for most economies, not a bane.

Bravado aside, Russia would certainly prefer oil at 110 dollars per barrel, but the reality is

[7] For those who remember the socialist time and its propaganda, импортозамещение is very familiar. Russian media regularly talk about all the unnecessary imports, replaced by the new products from Russia. If you watch the Russian state TV, you may think that all Western imported goods are gone from Russia by now. Only a nagging doubt would remain: if they managed this transformation in just 18 months, why haven't they done so in several decades?

[8] The Khanty-Mansijsk region produces 6 million barrels of oil per day. If it leaved the Russian Federation, it would have been the third largest oil producer in the world, after Saudi Arabia and the U.S.. Russia would have been behind it with 4 mbd remaining.

that it costs 50 dollars per barrel. The price can decrease. The journalistic question "can Russia survive oil at 20 dollars?" has a simple answer: yes. A more interesting question is what sort of Russia this would be.

With oil and gas providing 60 per cent of the state budget and oil making four fifths of this sum, it is not surprising that Russia is trying to calm the oil markets[9]. Rhetoric is one thing, default is a completely different story. Nobody at the Kremlin is willing to risk to repeat what happened in August 1998.[10]

GAS WEAPON. REALLY?

Theoretically, Russia could either target individual countries or threaten to completely cut off gas supplies to the West. Let us start with the possibility of targeting a single country or a group of countries.

On the face of it, Moscow has a whole set of options. Twenty-one EU countries[11] (if their gas companies are taken into consideration) buy Russian natural gas from the company Gazprom[12]. Most of them have comfortably diversified their portfolio of sources. Some import 100 per cent of their natural gas from Russia – among these, several have no other possible route for gas delivery.

However, a deeper analysis shows that their dependency on Russia is not so huge. The share of natural gas in primary energy sources is small in many countries, which means that the result of a gas cut-off would be fuel-switching, replacing gas with other fossile fuels. Also, countries which use a lot of gas have a back-up. (For example, Finland is able to convert its heating systems from gas to coal in several hours – and has strategic coal reserves to face an eventual gas cut-off). Most member states have sufficient level of diversification essentially due to multiple pipelines and several possible sources of natural gas.

Even more importantly, the European Union has made it crystal clear that an attack on any of its members would be considered as an attack on all of them. The EU has no Article V like NATO (the *Musketeer clause*, "One for all, all for one"), yet its credibility stems from the fact that it represents *all* its citizens amounting to half a billion people. It takes this matter seriously: the solidarity ethos is much more profound than a casual observer would recognise. Hitting a single country – for instance, Bulgaria or Hungary – would mean confrontation with the EU-28. The ongoing anti-trust case against Gazprom, which led to issuing the *Statement of Objection*[13] by the Commission on 22th April 2015, is a case in point. Therefore, Gazprom was targeted for trying to limit (or ban) reselling of its gas to third parties and to hike prices for countries with no other options (which are smaller deeds than cutting gas supply off to a country). In the end, Gazprom will either fully comply with the EU's Third Energy Package, or leave the EU market. *Tertium non datur*. The timing of this lesson was not lost in Moscow.[14]

This leads us to the possibility of a total Russian embargo on gas sales to Europe. That would take roughly one third of natural gas

[9] Russia has significantly increased its oil output since 1991, reaching the highest level of production in 2015 for the first time since the break-up of the Soviet Union. More precisely, Russia today produces as much oil as the U.S.S.R. did. This is impressive as the Soviet Union included other oil-producing republics, mainly Kazakhstan, Azerbaijan and Uzbekistan, apart from Russian Soviet Federative Socialist Republic (R.S.F.S.R.).

[10] The default of 1998 was one of the defining moments for Vladimir Putin's politics. It made possible his journey to the position of Prime Minister from relatively weaker jobs in security services (which in 1990s were, unlike today, not centers of power). He remembers the chaos of bankruptcy and the upheaval that followed.

[11] Finland, Estonia, Latvia, Lithuania, Poland, Germany, Netherlands, Luxembourg, Belgium, UK, Czech Republic, Slovakia, Austria, France, Hungary, Italy, Slovenia, Croatia, Romania, Bulgaria, and Greece.

[12] It has to be mentioned here that Gazprom's position inside Russian power circles has greatly diminished over the last decade. Back to the 1990s, Gazprom was the only foreign policy tool that Moscow had, since oil industry was mostly privatized (only a minor company called Rosneft was left in treasury). In 2003, the state dismembered the largest private oil company Yukos, with Rosneft being the biggest benefactor. It quickly become No 1. Since then, it has been Rosneft who has dominated the domestic energy scene, not Gazprom, because oil makes four fifths of the revenues and gas only one fifth. Some in Western media keep using the words "Russia" and"Gazprom" as interchangeable, but that's increasingly less true. We will probably see more changes in the coming years: there are new important gas producers (Rosneft, other oil companies, and Novatek) who are trying to break into the foreign market – which is still Gazprom's monopoly.

[13] Those that are not versed in the EU jargon laugh when they hear the term Statement of Objection. Ask Microsoft, Intel, or GE what they think about the European Commission and its anti-trust powers. There will be very little laughter.

[14] I would not, however, exclude the possibility of a full-blown confrontation with the Commission. Gazprom's response to the Statement of Objection was probably not written by Gazprom's lawyers, but by someone with a very particular view of the importance of Russia and its gas: "Gazprom…being established outside of the jurisdiction of the EU, is a company which in accordance with the Russian legislation performs functions of public interest and has a status of strategic state-controlled entity." Full text in English: http://www.gazprom.com/press/news/2015/april/article224444/

off the European market, perhaps for a long time. It is something we do not wish to happen, but which we are not too terrified of. The European Commission conducted a large excercise in summer/autumn of 2014, assessing the vulnerability of its member states to four different possible Russian cut-offs:

1. No gas through Ukraine for a month.

2. No gas through Ukraine for six months.

3. No gas through any export route (Ukraine, Yamal-Europe, Nord Stream + country-specific pipelines in the Baltic area) for a month.

4. No gas through any export route (Ukraine, Yamal-Europe, Nord Stream + country-specific pipelines in the Baltic area) for six months.

The first two variants would mainly hit South-Eastern Europe and parts of Central Europe, while the other two would add Germany, France and Italy, among others, to the hit-list.

In addition to the basic criteria, these stress-tests also studied several possible levels of cooperation between the EU member states: from "solidarity at all times" to "beggar thy neighbour".

The results, which were published before the winter of 2014/2015, were good. Only two members out of 28, namely Bulgaria and Hungary, would face significant difficulties in gas deliveries, and even in these two countries it would not be the end, thanks to the ability to switch to other fuels[15].

To put this more clearly: should Russia cut off its gas to Europe completely, it would be a difficult winter for us. Getting supplies from other sources (mainly Liquefied Natural Gas-LNG- from Qatar and Australia) could take months and sellers would probably ask for a premium. Replacing gas with other fuels (in the short-term mostly with coal and heavy heating oil) is costly, not to mention environmentally damaging. But it can be done – and it would be done. Europe is still the richest continent on the planet and it can deal with an emergency like this.

On the other hand, Russia would be out of its main market for at least a generation. It would not have any possibility to come back a year later saying "sorry, guys". Additionally, it would not be able to sell its gas to anybody else, since LNG projects are very much damaged by the EU sanctions. The only pipelines that Russia has in its main production area of Yamburg-Urengoy at the moment are the ones bringing gas to Europe (from the north of Finland to the south of Turkey).

If Russia wants to scare Europe – or, at least, to be taken seriously when threatening to leave the European market – it must be able to export its gas somewhere else.

LNG AND OTHER HI-TECH PROJECTS

The only way to break out of pipeline dependency is to build LNG terminals. This is what Qatar did, after its spat with Saudi Arabia – and it benefited the country very much. Russia has studied Qatari experience very carefully and has tried to emulate it, especially in regions like the Far East and the Far North. It has worked well – as long as there were Western[16] companies involved.

Then, the West imposed sanctions on Russia. Let me illustrate their impact by using the LNG example.

Sanctions have had a double impact. The first one is that many technological products are forbidden to be sold to Russia whose companies are not allowed to do business with the western ones. Additionally, banks have no access to global money markets. This has already happened, especially in the third wave of sanctions applied in the summer of 2014.

[15] Stress-tests also looked at non-EU countries importing Russian gas. Among these, Moldova and Serbia would face problems, but their resilience is high and (unfortunately) well tested. Serbia survived embargoes, sanctions and NATO bombing. Moldova went through a war and still does not control large part of its territory ("Trans-Dniestr Republic", which is another Russian frozen conflict).

[16] I include Japan in the „Western" group of countries. Japanese companies are very active in several projects in the Russian Far East, especially in Sakhalin.

The second impact is less-well documented, but equally harsh. Every large company that is Western-owned or dependent on Western lending and auditing has a compliance officer that is usually its chief legal advisor, sometimes even the Vice-President. If a manager wants to make a deal related to a sensitive region or to a protected technology, he or she asks the compliance officer for approval – who usually errs on the side of caution. Nobody wants to be investigated by SEC or FBI.

The definitions of "sensitive regions" and "protected technologies" are fuzzy. They might include components that common sense would see as harmless, yet when put together they could be declared dual-use or sanctions-breaking. If your company is doing fine, you will not risk everything (including your freedom) just to make few more dollars. Sure, business is business and sharp elbows are necessary. The ability to look the other way is a bonus. But there is also a risk, and everybody is well aware of it. There have been deal-makers who struck gold in proscribed areas and are now in U.S. federal prisons.

LNG falls precisely into this grey area. LNG trains have been used for commercial operations for more than half century, first in Algeria, then in many other countries, from the Persian Gulf to Trinidad, as well as in Indonesia and in Australia. The technology to squeeze natural gas 600 times while simultaneously cool it with a temperature of minus 162 degrees Celsius is well known since the 1940s. Yet only few companies can do it safely enough[17]. These firms are all based in Europe, USA and Japan, with customers around the globe and a wait-list of several years[18]. Doing nothing in Russia for a couple of years will not harm them. Russian share of the LNG market has been small so far (Sakhalin platform in Far East was built and few projects are planned in the Far North) and is unlikely to grow significantly until the current East-West stand-off ends.

ALL PIPES TO CHINA?

The discussion above explains why there was so much fanfare in Moscow for the new pipelines to China. In the summits held in 2014, Putin and Chinese President Xi Jinping announced the construction of two major pipeline projects bringing gas from Russia to China. One is *Power of Siberia*, which would bring natural gas from newly developed fields Kovykta and Chayanda in Eastern Siberia to the Middle Kingdom. The other one, originally called *Altai* and later on renamed *Power of Siberia II*, would connect the current major production area of Yamburg-Urengoy in Western Siberia to the Chinese market, giving Russia a possibility to thumb its nose on Europe.

Let us start from the last point: if Russia wants to replace twenty well-paying customers with a single, pretty tough buyer, good luck. Gazprom has no longer a monopoly in some parts of Europe, but its position is still better than having the Chinese monopsony.

Opening of new fields in Siberia is more difficult. I have already mentioned the *Lada versus Ford* dilemma. This is the case where it comes into full force. Kovykta lies five hundred kilometres at the north of Irkutsk, in the middle of nowhere. Chayanda is further north in the Sakha Republic (aka Yakutia, which must not be confused with Sakhalin Island, which is at the north of Japan). It is possible to open new fields here with domestic companies and domestic technologies – provided that there is Chinese funding. This is where the trouble starts.

There was a revealing moment at the Far Eastern Economic Forum in Vladivostok in September 2015. Its highlight was supposed to be the Russo-Chinese panel of major banks, launching new common projects. In the end, no project was mentioned. Instead, the representative of VTB, one of the largest Russian banks, criticized his Chinese part-

[17] I have been to several LNG facilities around the world and procedures were vigorously controlled in all of them, reminding me of nuclear powerplants with their stringent safety culture.

[18] Sabine Pass, Lousiana, USA, is a good example. The project costs roughly 20 billion dollars and is fully booked already, yet it is building LNG trains at a pace of one per year. "The suppliers can not deliver more than one at a time, they are stretched everywhere. The interest in LNG is too high at the moment", told me a manager of the site earlier this year.

ners for applying sanctions too scrupulously. In his words, things, which used to take hours to be decided, now take weeks and in the end they do not happen at all. He specifically pointed out Rosneft as a victim of this unfriendly approach. What he forgot to mention was the fact that both Rosneft and VTB are on the sanctions list. Chinese banks know too well that should they touch Rosneft or VTB, they would be cut off from access to cheap lending. Friendship is fine, good credit is better.

Interestingly, the only signing ceremony at the Far Eastern Economic Forum was organized for a project to be realized in Europe, namely Nord Stream 2.

TOO MANY STREAMS

One year ago, the only Russian project for the construction of new pipelines to Europe was the South Stream, running under the Black Sea to Bulgaria and through the Balkans to its main destination, Italy. Later, on the 1st December 2014, President Putin visited Turkey. He anounced that the South Stream project was cancelled and that Gazprom would build the Turkish Stream pipeline to Turkey. The Turkish Stream was considered as very important during the spring of 2015, but it was quietly put aside in summer that year. In June 2015, the enlargement of the existing Nord Stream pipeline was announced. The new pipeline was called Nord Stream 2 (also Nord Stream 3+4; it is supposed to add two more pipes to the existing lines 1+2).

The polite description of this should be "frantic activity". No matter how you look at it, it does not give the impression that Russia wants to leave its most important market. We sometimes forget that Gazprom exports only one quarter of its gas. Yet, this provides 95 per cent of its profits.[19]

The big question here is whether Russia will keep transiting its gas to Europe via Ukraine after the current contract will expire in 2019. Nobody knows: there is a war between Russia and Ukraine, although undeclared, and their relationship is going to be bad for quite some time. The transit via Ukraine could end tomorrow, or stay in place well after 2019. Both outcomes are possible and Europe is ready for both possibilities. We would prefer to have more delivery routes from Russia (read: keep Ukrainian transit), but our main focus is on diversifying our suppliers. Russia is no longer the EU's biggest supplier of gas via pipelines. Norway has overtaken it recently. No surprise here. My country, the Czech Republic, has a contract for gas with Norway since 1997. It has always been a straightforward and clear deal, with Norvegians sending gas as agreed and we paying on time. No fuss, no crisis, no blackmail. Just gas.

STAY UNITED – AND PATIENT

We have rarely known a theory that has been so thouroughly debunked in such a short time like the *Russian energy weapon*. In one and a half year since the occupation of Crimea and the resumption of the East-West contest, Russia has tried to play this card – with minimal results. Clearly, energy is only a part of the economic power of a country, and energy security is only a component of the broader stability/security of the realm. States with plentiful resources, but shabby economy (such as Venezuela, Nigeria and Russia) have very little sway over their more developed counterparts.

What Europe – and the West in general – needs to do is to keep its current approach. Diversification of suppliers, as well as of supply routes, has been our main strategy for decades. Building inter-connectors between member states and creating a single market of 500 million people are both smart and prudent. It is equally important to let our beloved suppliers understand that we are polite, but not meek – hence the importance of the anti-trust case against Gazprom.

Russia's energy weapon exists, no doubt about it. Yet, we are the ones who are winning.

[19] An important number to remember is the following: Russia burns roughly 450 billion cubic metres of gas (bcm) per year. Germany, with much higher GDP, uses 90 bcm. What you can blame for is the cold weather.

Energy in New Generation Warfare. Learned lessons from Russia's hybrid war against Ukraine

Mr. Mykhailo Gonchar and Mr. Andrii Chubyk, Centre for Global Studies Strategy XXI, Ukraine

Energy has become one of the main targets in modern warfare because of massive introduction of machines and engines to increase the power of destruction. However, for a long time, targeting energy supply and infrastructure has been a secondary task in comparison to conventional warfare. The situation changed during the Cold War as the Soviet Union made the famous "gas for pipe" deal1 with Germany, which meant the energy dependence of Western economics on Eastern supplies.

The collapse of the Soviet Union, defined by Russian President Vladimir Putin as "the biggest geopolitical catastrophe of the 20th century"[2], has not changed Russia's plans to use energy as a political and military tool. Prolongation of the Russian Black Sea fleet stationing in Sevastopol in 1997 (gas for debts), the gas crises of 2006 and 2009 and the Kharkiv agreements of 2010 (gas for fleet until 2042) are the only Ukrainian cases of energy component deployment by Putin's regime. After the open military aggression of 2014, Putin activated an energy offensive by cutting gas supply, threatening European Union (EU) suppliers with gas limiting and ordering massive destruction of energy infrastructure in Ukraine. All these instruments can be used to exert pressure also on other countries and are presented in this re-

Mr. Mykhailo Gonchar, Centre for Global Studies Strategy XXI, Kiev

Mykhailo Gonchar is the President of the Centre for Global Studies "Strategy XXI", an independent Ukrainian think tank dealing with research on energy issues. His professional interests include international energy policy, energy security, transparency, international relations, and global security developments. In the 1990s, Mr. Gonchar served in the National Security and Defence Council of Ukraine, did internships at the European Commission and NATO, worked as research fellow at the National Institute for Strategic Studies, and at the National Institute of International Security Problems (NSDC) in Ukraine. In the 2000s, he worked in the oil and gas complex system of Ukraine. Since 2007, Mr. Gonchar has been working as independent expert. He is the author of several books and numerous articles on issues related to energy, energy security, and international relations. He has published in Ukraine, Poland, Slovakia, Germany, Great Britain, Turkey, the Netherlands, and Finland. He has worked as rapporteur and moderator of a number of international conferences on energy and security issues in Poland, Slovakia and Germany.

[1] Stern,Johnatan, Gas pipeline co-operation between political adversaries: examples from Europe, Report Submission to Korea Foundation, Chatham House, January 2005, available at https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/Energy,%20Environment%20and%20Development/jsjan05.pdf

[2] Владимир Путин: "Распад СССР - крупнейшая геополитическая катастрофа века", in Regnum, 25th April 2005, available at http://regnum.ru/news/444083.html Любое использование материалов допускается только при наличии гиперссылки на ИА REGNUM.

search together with analytical conclusions and predictions.

After the collapse of the Soviet Union, only central European states could join the western institutions, namely the European Union (EU) and the North Atlantic Treaty Organization (NATO). By contrast, eastern European states (Ukraine, Moldova and Georgia) were excluded from the enlargement process of those institutions. The willingness of excluding them from the EU and NATO enlargement process was very clearly shown by the position of Germany and France in the NATO Bucharest summit in 2008. The EU's attitude towards eastern Europe has indeed always been the same since the Soviet era, which means that the EU has not applied its values to this part of Europe leaving them apart while pursuing its economic and geopolitical interests. For instance, European values (rule of law, democracy, human rights) have never played a decisive role in business relations. This is especially true in regard to Russia, whose values do not coincide with the EU ones. Many EU countries have benefited from corrupted money coming from Russian post-soviet ruling clans. Even the evident violation of the international law by Russia in Georgia has not prevented the EU from endorsing the "Partnership for Modernization" in 2010. Additionally, the EU has imposed only moderate sanctions to Russia in response to its annexation of Crimea in 2014. This has reinforced Russia's idea that the West is "weak and infirm". At the same time, Russian warfare in Donbass has strengthened Kremlin's gangster-style politics attitude against the West with the aim to change the world order. In this context, Russian President Vladimir Putin uses energy, which is one of the most important Russian resources, as a foreign policy tool.

Energy is an important component of the Russian version of the New Generation Warfare. This is a complex of diverse controlled and combinable effects on the enemy obtained by breaking this latter's resistance without fighting.[3]

From the Kremlin's point of view, the basic determinants of Russia's geopolitical strategy of the 21th century can be formulated as follows: the ones possessing self-sufficiency in terms of resources (e.g. energy, water, food, and minerals) and of power (e.g. nuclear weapons, organizational weapons, energy weapons, and cyber forces) can rule the world.

Russian conceptual approach to organizational weapons is explained in a report by the Izborsky Club-Dynamic Conservatism Institute. It defines organizational weapons as "a way to establish a pathological system in the target-state, so that the former consumes the resources of the latter for

Mr. Andrii Chubyk, Centre for Global Studies Strategy XXI, Kiev

Andrii Chubyk is the Executive Director of the Centre for Global Studies "Strategy XXI". His professional interests include: energy sector development, international energy policies and international relations, sustainable development, energy transparency and energy security. Mr. Chubyk has participated in several academic programs, namely Warsaw Euro-Atlantic Summer Academy (Warsaw, 2013), Revenue management and economic diversification in petroleum rich countries (Baku, 2013), Goerdeler-Kolleg for Good Governance (Berlin, 2012) and others. He is the author of a number of publications on energy related issues in foreign and national media sources. He has worked as acting expert on energy issues for the Civil Society Forum of the Eastern Partnership programme, WG3 "Environment, climate change and energy security", and he has participated in the Multi-stakeholder group on Ukraine's joining Extractive Industries Transparency Initiative. He's co-editor of the information web-resource www.geostrategy.org.ua

[3] Berzinš, Janis, The New Generation of Russian Warfare, Aspen Institute, available at http://www.aspeninstitute.cz/en/article/3-2014-the-new-generation-of-russian-warfare/

its development. A characteristic feature of the pathological system (application of organizational weapon) is that it affects the functional system of the society from the 'outside', from a hierarchical 'overlying' (powerful) level of system organization".[4] Additionally, the report stresses that "the use of organizational weapons 'is not always evident' to the traditional forms of scientific observation and is 'incomprehensible' through the traditional logic of everyday cognition. Destruction, as the action of organizational weapons, aims at achieving results that are in the "system of values" of the initiator applying the weapons. One of the main conditions for the application of organizational weapons is the substitution of the basic values of the target-state with the values of the initiator-state".[5]

Two prominent examples could serve as a clear explanation of how organizational weapons are used. The first one is the official statement[6] highlighting that the development of economic cooperation between Russia and Ukraine is a priority issue in the relations between them. However, this statement was not followed by facts. The real aim of Russia was indeed to create increasing dependence of Ukraine in economic and (geo)political terms. In particular, growing gas dependency serves this goal. It has exhausted the state finances and has created debts for the country. It has increased the Russian political pressure on Ukraine also through the "take or pay clause" included in the gas contract fixing gas volumes and envisaging politically motivated changes of prices.[7] This clause creates trade imbalance in favour of the aggressor, implies the possibility of trade wars and boycotts against the victim-state for political reasons, and promotes corruption among politicians and oligarchs.

The second example is the false message spread by Kremlin's political and diplomatic circles after the bloody clashes with the Russian army in Donbass: "Ukraine and Donbass need a peaceful dialog". As peace is a universal value, it was expected to obtain predictable responses from Kyiv, Brussels and Washington. Counterreplies were actually also expected. For Brussels and other EU capitals a "military solution does not exist." Ukrainian President Petro Poroshenko stated "I am a President of Peace, not of War". For Washington "a diplomatic solution" was necessary. Differently from the meaning they have in the West, "humanitarian convoys" transporting ammunitions became a symbol of Russian "peace efforts". The culmination of the "peace efforts" of the parties involved (namely Ukraine and Russia) was the defeat of the Ukrainian Armed Forces in Ilovaisk followed by Minsk-1 agreement in September 2014. In February 2015, everything occurred again in Debaltsevo and Minsk-2 agreement was signed. Everyone keeps talking about peace, which however does not occur, although there is a decrease in the intensity of the fighting.
Russian hybrid aggression against Ukraine has smoothly and gradually transformed into a training phase of intrawar. Intrawar is an internal war based on the civil conflict triggered and fueled from the outside, where an aggressor takes part minimally and in hidden way through subversive troops and local organizations, as well as through "volunteer formations" and groups of foreign mercenaries. Local elections held in Ukraine on 25th October 2015 should become a touchstone and a checking point for Russia to estimate the effects of this kind of aggression.

Differently from what happens in the Western democracies, Putin's Russia is very prone to engage in various conflicts and to use all

[4] Организационное оружие: Функциональный генезис и система технологий XXI века (доклад Изборскому клубу), Izborsky club, available at http://www.dynacon.ru/content/articles/1466/
[5] Ibidem
[6] Договір про дружбу, співробітництво і партнерство між Україною і Російською Федерацією, Verkhovna Rada Ukraine, available at http://zakon5.rada.gov.ua/laws/show/643_006
[7] "The take-or-pay clause requires that gas has to be paid whether taken or not, and specifies an obligation for the seller to make available defined volumes of gas (though make-up provisions allow carrying forward to a later year gas paid for in one year but not taken)".
Creti, Anna, Villeneuve, Bertrand, Long-term contracts and take-or-pay clauses in natural gas markets, University of Toulouse, October 24, 2003, available at http://www2.toulouse.inra.fr/lerna/cahiers2003/0310116.pdf

kinds of instruments including sabotage, terrorists, trade boycotts, blackmail, military and diplomatic tools. Also, the utilization of energy assets for political purposes is Putin's long-term strategy. Several documents prove this attitude, as for instance:

• "Russia possesses huge energy resources deposits and a powerful fuel energy complex, which is the base for the development of its economy, an instrument of foreign and domestic policy implementation" (2003, Energy Strategy of the RF till 2020);

• Mikhail Margelov, a special envoy of the Russian President to Africa and a Chairman of the Foreign Affairs Committee of the Council of the Russian Federation very openly expressed his opinion on the instruments of Russian foreign policy in November 2011: «... oil and gas policy should become not only a significant part, but one of the most important instruments of the Russian foreign policy».

• The following recommendations contained in the updated Energy Strategy of the Russian Federation until 2030 are very effective in revealing Russia's conceptual approach to energy: «...the main priorities of energy policy for the concerned period are <...> effective deployment of Russian energy potential with regard to international economic and political relations <...>, ensuring the geopolitical and geo-economic interests of Russia in Europe and in the neighboring countries, as well as in the Asian-Pacific region»[8].

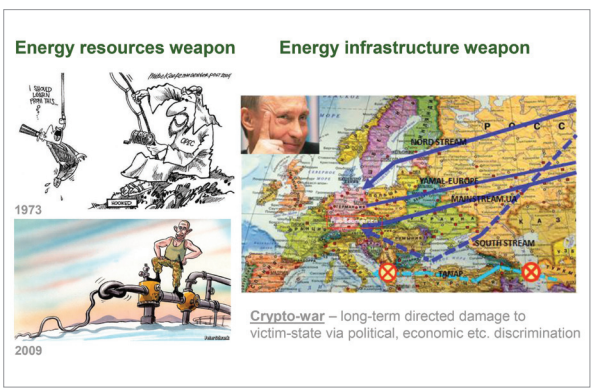

Figure 1. Energy weapon. Energy warfare. Crypto war

• When formulating the basic provisions of the Project Energy Strategy until 2035, Russia introduces an additional dimension of its external energy policy: «Russia as a responsible state considers its external energy policy not from the exporter's narrow point of view, intended to maximize short-term revenues, but as a tool to solve both national and global problems»[9].

Two cases of Russian "gas aggression" against Ukraine in 2006 and 2009 respectively can be considered as the implementation of Russian foreign policy in its neighbouring countries. Europe used to call them "Russia-Ukraine gas crises", which reflects the traditional unwillingness of the European Commission to call things by their proper names. Cutting off gas supply to Ukraine and reducing the volumes of gas transit via Ukraine to the EU in 2006 were Russian "actions of punishment". Ukraine was punished for the Orange Revolution in 2004, Europe for supporting Ukraine. Now it can be concluded that it was the use of the gas shortage due to cut off deliveries from Russia in the long phase of Crypto-war (intended as a *covert form of gradual, systematic and long-term endamagement of the victim-state in order to maximize the exhaustion of its potential, until a decision about aggression of hybrid or classic type is taken*), which had to go to the stage of hybrid invasion.

The crisis of 2009 had far-reaching goals for Russia. It should provoke a political conflict in Ukraine along the axis East – West. It aimed at causing gas shortage in the eastern part of the country by totally disrupting gas supplies (both for domestic and EU consumption). In so doing, Kiev's authorities would be unable

[8] Energy Strategy of the RF Concept till 2030 (project). Institute of the Energy Strategy, available at http://www.energystrategy.ru/editions/concepc.htm
[9] Energy Strategy of Russia for the period till 2035 (basic provisions), Institute of Energy Strategy, available at http://www.energystrategy.ru/

to deliver gas from the Underground Gas Storages (UGS) located in the western part of Ukraine to the main industrial centers, which would have no heating at disposal. According to Russian strategists, it should provoke a "social explosion in the East and the South of Ukraine". In 2009, the Russian Strategic Culture Foundation studied the so called "half hard" scenario, which occurred to face the emergency situation. Therefore, the military contingents to Ukraine were deployed and a "provisional government" was established, while the local self-government authorities were distributed on the occupied territories with reliance upon well prepared "support forces" – marginal groups with critical approaches toward Kiev-based authorities and the creation of "independent" quasi-state institutions" in the country. In this context, it was not a case that on the 12th of January of that year the Russian mass media published an article on the topic "borders revision" in the Commonwealth of Independent States (CIS) including statements of Russian politicians such as the following: «Member of the State Duma of Russia Konstantin Zatulin does not rule out the fact that Russia can "signal at the proper moment" to the eastern and the southern regions of Ukraine to join Russia»[10]. This scenario failed the same year because the Ukrainian gas transportation system reversed gas supply: the central, eastern and southern regions of Ukraine received gas from underground gas storage.

In 2014, Russia used energy as a tool of its foreign policy again as gas supply to Ukraine was disrupted for 180 days. Additionally, coalmines and transportation routes were destroyed, and thermal power plants close to the warfare line were attacked with artillery and rockets.

Russia created two alternatives for Ukraine: the shortage of coal should be covered either by importing it from the Russian Federation or by buying it from so called Lugansk People's Republic and Donetsk People's Republic in Donbass controlled by Russia. Nevertheless, Russian "coal leverage" could not be used effectively as occupied Crimea depends on electricity supply from the United Energy System of Ukraine for 85%. Ukraine used this to deter Russia from advancing into the Donbass territory. Indeed, it demonstrated what could happen in case of further aggressor's offensive by disrupting the electricity supply to Crimea on 25th-26th December. On 30th of December, some energy companies (Національна енергетична компанія "Укренерго", Національна компанія "Крименерго") signed some agreements, which benefited both Ukraine and Russia. They guaranteed coal supply to Ukraine and uninterrupted supply of electricity to Crimea. Thus, both parties used energy leverage in the conflict.

The use of energy as a weapon is effective when supplies depend on other countries and when there are surplus of pipeline capacity, high energy prices, low temperatures in winter, as well as increased energy demand. In the case of Russia-Ukraine 'gas war' the strategies used by Russia have been inefficient because of the reduction of gas prices since the summer of 2014, the warm 2014-2015 winter, and the reverse gas supply from the EU. Additionally, over the last few years

Vuglegorsk, Donetsks region

Nebyliv, Ivano-Frankivsk region

Means: fougasse, rocket artillery Grad type, heavy mortar, long-range artillery

Targets: main and medium pressure gas pipelines, transformer units, electricity lines and distribution points

Figure 2. Warfare on critical energy infrastructure

[10] Затулин о Хмельницком, Ющенко и знаке в нужный момент, The UNIAN, January 12, 2009, available at http://www.unian.net/world/179446-zatulin-o-hmelnitskom-yuschenko-i-znake-v-nujnyiy-moment.html

there has been a reduction of gas consumption in Ukraine. Cut of gas imports from Russia was even more dynamic (2014 – 14,5 bcm, 2015 – 6 bcm, following a rapid increase in the volumes of gas deliveries from the EU countries through reverse).

Differently from what happens in the case of gas, in the electric power sector there are not any possibilities of resorting to reverse of gas supplies from the EU. An option would be to use the electric power of the "Burshtyn energy island", which is located in the western part of the country and which operates as a stand-alone electricity source for exports to the countries of Central Europe. It can be exploited to supply the United Energy System (UES) of Ukraine. Additionally, since summer 2015 the nuclear energy capacity of Ukraine has increased. For the first time in the history of the country, the electricity produced with nuclear energy exceeded the one produced with other types of energy. The electricity production amounted to more than 60% of the total volume, much more than the average production corresponding to 48%.

However, these measures can be insufficient in extreme cold weather conditions. In this case, Ukraine might be forced to turn to Russia for additional import of electricity. Like in the case of the scenario described above for the gas sector, Russia can impose harsh conditions to provide electricity to Ukraine. The core idea would be to apply the formula "gas and electricity in exchange of the recognition of Crimea as a Russian territory and of a special status for DPR/LPR". Undoubtably, Russia would try to use the "electric trump card". In summer 2015, it was conceived a scenario in which the Moldovan thermal power plant located on the territory of Transnistria controlled by Moscow would stop providing electricity supply to the southern part of Ukraine (the Odessa region).

Ukraine is able to withstand the Russian energy blackmail through the political will of its leadership. Total blockade of the occupied territories of Crimea, Donbas, and Transnistria might be adequate countermeasures against Russian presumption. Also, it is important that the government of Ukraine approved the "Plan for the preparation of the fuel and energy complex of Ukraine for the autumn-winter period 2015 - 2016 and its passing" in early August 2015.

Being an expert tactician, Putin tries to exploit the ongoing situation in Syria to change the attitude of the West towards Russia and its involvement into warfare in Ukraine. In so doing and by multiplying the problems for the West, Putin aims at reaching several objectives:

• Shifting the attention away from Ukraine to the Middle East and focusing its own capacities on a quasi anti-ISIS operation;

• Providing support to the only ally Bashar Assad and destroying the potential route of the Arab gas to the European market;

• Maintaining and strengthening its status of monopolistic provider of hydrocarbons to Europe from the East and promising good business for European energy companies within the Nord Stream II project;

• Obstructing the current and prospective non-Russian supplies to the EU (the Caspian region and Central Asian countries should be

Figure 3. Warfare on critical infrastructure

aware of the middle range rocket type Caliber (NATO code Sizzler) firing from Caspian Sea on October 7, 2015);

• Obstructing prospective bypassing routes for hydrocarbon supplies to Europe (for instance, the Trans-Anatolian Natural Gas Pipeline-TANAP- by hidden stimulation of the Kurdish issue in Turkey, Syria and Iraq with already occurred explosions on Turkish territory in summer 2015);

• Having under its direct or indirect control the unexplored hydrocarbon deposits that are very rich of energy resources (e.g. the Arctic deposits and the Black Sea ones in Crimea).

On the 4th September of 2015, Gazprom and several European energy companies signed an agreement concerning the construction of the Nord Stream II pipeline. Therefore, Russia and, at least potentially, the European companies that have signed the agreement could be willing to provoke a third "gas crisis" in winter 2015/2016. They could be interested in showing the EU authorities that Ukraine is an unreliable transit country of Russian gas from Siberia and in convincing them to approve grants for full-fledge utilization of existing and future Russian pipelines.

The annexation of Crimea and the invasion of the East of Ukraine have served Russian strategic goals. Some examples are the breakdown of major projects concerning the development of natural gas deposits in the Black Sea and the development of unconventional gas onshore, which have been important for both Ukraine and Western companies. As a consequence, European and American companies left the country.

The Caspian region and the Southern Caucasus are potentially critical regions as companies aiming at developing projects concerning gas transportation in these regions are competing for Russian deliveries to Europe. This is why the possibility of a military intervention of Russia cannot be neglected. It is worth noting that if this case concretely occurs, the involvement of EU and NATO in these regions would be helpless, unless they opt for preventive actions in the near term to deter Russia.

The USA and NATO should pay serious attention to the security dimensions of the Caspian region, the South Caucasus, and the Euro-Arctic region. Considering the features of Russian policy described above, it is not possible to neglect the possibility of a renewal of the Armenian-Azerbaijani war, which would transform the South Caucasus and the Caspian regions into a high-risk zone since several projects for production and transportation of gas resources to the EU are foreseen in those areas. It is necessary to strengthen the regional intelligence capabilities of NATO in the Caspian Sea, the South Caucasus, the Black Sea, the Baltics, the Arctic, as well as in Russia, Belarus and Kazakhstan – where there are energy resources, which Russia sees as strategic for its national geopolitical and economic goals. It is important to follow and evaluate the activities of Kurd militant groups in Turkey, which are responsible for several attacks on pipeline infrastructure occurred in July and August 2015. A special attention should be paid to cyber space activities with regard to smart grids in Europe especially in periods of low temperatures during the winter 2015-2016.

It is evident that Russia ruled by President Vladimir Putin is not a partner neither for the West and Ukraine nor for any other country in the world because of its conception of international order and cooperation. Having misused the chance to modernize Russia through enormous energy revenues in 2000th, Putin desperately attempts to show Russians that they are still living better than other nations, while breaking peace and trust in the country at the same time. He can save his "own face" only by defeating the "decaying West", meaning the collapse of the EU and NATO because of their inability to manage multiplying crises.

Critical Infrastructure Protection: the challenges connected to working out the Green Paper on CIP in Ukraine

Dr. Oleksandr Sukhodolia,
National Institute for Strategic Studies, Ukraine

SITUATION IN UKRAINE

Ukraine used to have a well-developed, state initiated and strongly coordinated system of physical protection of critical infrastructure (CI) objects. However, the system was developed for the model of centralized governance focused on physical protection of important industrial objects and transport infrastructure for peacetime. The political and economic reforms in Ukraine, the emergence of new actors and the threats to CI have stimulated the changes in this field.

In addition, the development of the Critical Infrastructure protection (CIP) concept by some countries (like USA) in order to react to growing unconventional threats to CI demonstrated the necessity and urgency to change the methods of protection.

Development of powerful nuclear energy sector had obliged Ukraine to satisfy the international standards on protection of nuclear facilities. Following up international efforts on development of reliable system for physical protection of nuclear facilities and materials[1] (led by MAGATE) gave additional push to develop new CIP system in Ukraine.

The first deep research of the problem was conducted by the National Institute of Stra-

Dr. Oleksandr Sukhodolia, National Institute for Strategic Studies, Ukraine

Oleksandr Sukhodolia holds a Ph.D (1998) in electrical engineering and PhD in Public Administration. Sukhodolia has extensive experience in public service and higher education. He served as a Head of Department and Deputy Head of State Committee of Ukraine on Energy Conservation (1998-2003), Deputy Head of Energy Security Department at the NSDC of Ukraine (2007-20011). In 2001 - 2013 he was teaching energy efficiency and energy policy at the Energy Saving and Energy Management Institute.

At present Oleksandr is a Head of Energy Security and Technogenic Safety Department at the National Institute for Strategic Studies, office of the President of Ukraine. He is a professor of the National Academy of Public Administration.

[1] The system of physical protection system of nuclear facilities and materials is well developed in Ukraine and approved by MAGATE that creates possibility to transfer knowledge and best practice on other types of CI.

tegic Studies (NISS) of Ukraine in 2012 (D.Birykov, S.Kondratov, 2012).[2] This publication became a starting point for the development of a new governmental policy on CIP - the Green Paper (GP) on CIP.[3] The first draft of the GP was presented by NISS in 2014 and it was followed by expert discussion. Work on the GP was carried out by the NISS with the active participation of domestic and foreign experts - support from NATO Liaison Office in Ukraine and NATO Energy Security Center of Excellence.

The final draft of the GP was presented by NISS in October 2015. This document reflects our current understanding of importance of CI stable functionality and its' impact on national security.

THE MODERN PROBLEM OF CIP

The new type of warfare, launched by Russia against Ukraine in 2014-2015, requires rethinking of the whole CIP paradigm. The reality is that targeted malicious actions against critical energy infrastructure (CEI) could constitute a state strategy of warfare strategy against other country (O.Sukhodolia, 2015).[4] the Analysis highlights the emerging threats of new types of war - "infrastructural war" that targeted to influence population (not defeating by army forces) of countries under attack. It highlights another feature of this new situation, - the more technologically, institutionally and economically developed a country is, the more vulnerable it becomes.

TASKS AND PRIORITIES

The concept of the GP shapes the CIP system with focus on shifting government and public attention from "reactive" policy, removing crisis results, to crisis's prevention, emergency planning, strengthening coordination of different actors involved and establishing close public- private partnership relations. Shortly, eight important points are fixed by GP on CIP:

1. Including the expression "critical infrastructure"[5] into the legislation. Currently, the absence of the term leads to confusion in the lists of objects needed to be protected and creates difficulties in the effective coordination of efforts between different agencies.[6]

2. Defining the purpose of CIP, namely "to ensure a stable functioning of infrastructure" which guarantees supply of goods and services vital to the population, society, business and government.

3. Shifting the emphasis from the currently dominating dimension of physical protection of systems and facilities to the functions and services they provide.

4. Specifying the categories of threats according to the causes (*natural disasters, emergencies and technical failures, malicious activities*) and the elements of CI that the threat can damage (*physical elements, management and communication systems, facilities, personnel*).

5. Setting three goals of CIP that the system has to ensure:

- **a.** smooth functioning of CI (*reliability*),
- **b.** ability to resist against the threats (*resistibility*).
- **c.** ability to recover operations in case of interruption within a certain time period (*resilience*).

[2] D.Birykov, S.Kondratov. Critical Infrastructure Protection: problems and perspectives of implementation in Ukraine. Kyiv, NISS, 2012, 57 p. (in Ukrainian). Access: http://www.niss.gov.ua/content/articles/files/zah_ynfrastr-b98c0.pdf

[3] Green Paper Critical Infrastructure protection. Available at: http://en.niss.gov.ua/content/articles/files/Green-Paper-engl-4bd7c.pdf

[4] O. Sukhodolia. Problems of CEI protection in hybrid war. (in Ukrainian). Available at: http://www.niss.gov.ua/articles/1891/. See also O. Sukhodolia, "The energy dimension of war: overview of 2014-2015 Ukrainian events" (in English) expected to be published at Energy Security: Operational Highlights №11

[5] GP propose next definition of CI "Critical infrastructure is systems and resources, physical or virtual, those provide functions and services, disruption of which will result the most serious negative consequences for the vital activities of society, socio-economic development, and the national security of Ukraine"

[6] Ukrainian legislation regarding the protection of objects which, according to international practice, referred to as critical infrastructure is sufficiently branched and includes many regulations, which, however, are mostly of departmental character. Up to now, Ukraine has 15 different categories of objects with special conditions, to ensure protection and operation.

All these aspects should be reflected in contingency planning of CI operators.

6. Establishing clear governmental criteria to determine certain facilities and systems as CI.[7]

7. Predefining:

- operational regimes of CI (procedures) and modes of control of CIP system (both at a state and CI operator levels);

- related organizational, institutional, economic and law regimes of CI facilities functioning in accordance with levels of threats.[8]

8. Designing institutional and organizational structure and responsibilities of the involved parties.

Any changes in existing system and concepts, achievement of new set of targets is very challenging task for every country, but for Ukraine changes in condition of war is extremely difficult.

THE CHALLENGES IN CIP DEVELOPMENT

From scientific research, the GP project was transformed into practical activity to change governmental policy in Ukraine on CIP due to unexpected aggression from its former strategic partner.

The planned pace of GP development and practical the implementation of its provisions were accelerated due to the start of "hybrid war" against Ukraine. In addition, new tools of warfare stipulated the need to reassess the paradigm of CIP in Ukraine. This situation shows the lack of experts capable to accomplish established tasks due to limited timeframe, emergency, lack of resources and knowledge in the field of activity.

Another problem is the need to specify the role/place of CIP actions and responsibilities of involved actors in implementation of CIP concept. It has serious implication for interagency coordination and competition for "influence" in current structure of governmental bodies. The most relevant to CIP issue is that some systems of protection have been established in Ukraine:

- The Unified System of Prevention, Response and Suppression of Terrorist Acts and Consequences Mitigation (antiterrorist system);

- The Unified State System of Civil Protection (civil protection system);

- The System of Physical Protection of Nuclear Installations and Materials (physical protection system).

Now is hardly possible to change radically the current institutional structure in Ukraine. Therefore, GP propose to list and differentiate the whole scope of events related to CI malfunctioning to existed systems. So, ***"unintended events"*** like technical errors, accidents, natural disaster, etc. could be managed with the help of existing civil protection system while ***"targeted (malicious) actions"*** require the development of "prediction" and involvement of tools to react on terrorist treats[9] designed to cope with terrorist activities.

From the formal point of view, the adoption of such approach partially solves the problem of coordination in the field of CIP, especially in the cases of emergency. However, it is impos-

[7] The following characteristics may be considered as a factors that help to evaluate CEI facilities importance: scale of influence; infrastructure connectivity; time of occurring; object vulnerability; consequences severity (economic loses, internal and state security, psychological, safety of life, defense capacity, environmental safety)

[8] In terms of CEI there could be proposed next modes of CI functioning and CI protection system control regimes:
"Green" (threats identification) - normal functioning of infrastructure, regular application of CI protection system; - normal legal and economic regimes;
"Yellow" (threats determent) – warning functioning of infrastructure, expansion of the internal protection of external resources in order to prevent threat realization: - normal legal and economic regime with alert level of internal protection system;
"Orange" (threats suppression) - restriction on functioning of infrastructure, attracting external forces to eliminate threats; - restrictions in legal and economy regimes, involvement of external resources (similar regime was introduce on electricity market in Ukraine in winter period of 2014/2015);
"Red" (threats elimination) – changed modes of operation of infrastructure, control of external forces over process of eliminating threats and restoring functioning of infrastructure. – special legal and economics regimes (period of warfare Ukrainian legislation)

[9] The Law of Ukraine "On fight with terrorism". (in Ukrainian). Access: http://zakon2.rada.gov.ua/laws/show/638-15

sible to establish a comprehensive CIP system totally based on one system, like existing system of civil protection, because of methodological limitations.

There is another unsolved issue – the need to create a unified governmental system of detection and prevention of cyber-attacks against critical information infrastructure facilities, assess the level of security of its elements, and create counter-cyber capabilities as well as management and coordination for critical infrastructure.

Preliminary analysis indicates that the best organizational approach consists of creation of national and sectoral situational centres as a part of the national network of distributed situational centres (crisis centres of different systems) tasked with informational and analytical support by the National CIP Situational Crisis Centre. The added value of CIP system is to present institutional basis for "preventive planning" to secure CI stable functionality and resilience.

All above mentioned interdependent problems together create another very complicated management challenge, specifically overcoming the traditional understanding of activity (habitual routine and traditional procedures) from governmental bodies as well as operators of CI, namely:

- change habitual practice of involved actors activity;
- develop new set of legislation under time and resource constraints;
- redistribute the flow of financial and material resources;
- get new knowledge and skills;
- ensure mutually supporting actions of all involved actors (state, public, industry).

UPDATES AND ACHIEVEMENTS

The urgency of CIP problems became supportive by establishing general understanding of needed improvements. In fact, directly involved governmental agencies support GP development as well as following legislation needed for its practical implementation.

At present there is consensus on the need to implement contingency planning and risk management concept[10] into Ukrainian legislation and practice of governance with the aim to prevent interruption of CI functioning.

The set of main elements and formal tools of CIP system is already designed and partially approved too. The following tools are: "Design basis threat"[11], "Preventive Action Plan", "Emergency Plan", "Communication System (information exchange and efforts coordination)", "Training".

The **"Design basis threat"** (**"Projected threat"** in Ukrainian legislation) was approved by National Security and Defense Council (NSDC) of Ukraine in 2009 and later amended to have "Object projected threat" for list of objects.

The **"Preventive Action Plan"** on CIP developed by operators, agreed and approved by the relevant governmental authorities as well as "National Preventive Action Plan" must contain the detailed description of measures to identify and mitigate threats in different areas.

The **"Emergency Plan"** on CIP must contain the detailed description of recovery measures in case of crisis. The practice of emergency planning is well developed in Ukraine, especially in the civil protection system.[12] There should be improvements to address issues of interconnectivity and interchangeability of CI as well as changes in CI functioning regimes.

The **"Communication system"** (information exchange, efforts coordination) is well devel-

[10] Order of Cabinet of Ministries of Ukraine №37 from 22.01.2014 (in Ukrainian). Access: http://zakon1.rada.gov.ua/laws/show/37-2014
[11] The "Design basis threat" - the attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal or sabotage, against which a physical protection system is designed and evaluated (MAGATE- INFCIRC/225/Revision 5).
[12] Civil Protection Code. The Law of Ukraine. (in Ukrainian). Access: http://zakon3.rada.gov.ua/laws/show/5403-17

oped in a framework of physical protection of nuclear facilities system[13]. Proposed communication procedures contain certain formal elements on different levels of responsibility. Among important elements of the communication system there should be plan of interaction of central and local authorities on physical protection that requires:

• **Regional plan** for actions on physical protection, which regulates the involvement of military units and other law enforcement agencies of a region;

• **Object plan** for action on physical protection developed upon requirements of "Object projected threat", which regulates interactions of involved actors on object's level;

• **Communication and interaction procedures**, which establish requirements for format of interaction of agencies, clarify responsibilities of the agencies involved into acting in accordance with object and regional plans, timing of actions.

The **"Training"** exercises, which have to be designed to practice tactics of involved forces, to improve their skills, to check performance of tools.[14] The goal of training is to ensure the readiness of forces and tools of involved agencies to perform needed actions and procedures.

LESSONS LEARNED AND SUGGESTIONS

The process of GP on CIP development helps to identify the elements needed for a successful work:

• *Involvement of experts from the private sector and state agencies in drafting the CIP system*

It helps to shape right ideas of the GP as well as create support in order to facilitate "transfer" of new concepts into public entities activity. At the same time, it helps clarify provisions and escape legal traps and create common understanding of future cooperation between institutions.

• *Finding the added value to the existing structure and institutions*

Some threats to the stable functioning of CI could be generated by malicious actions, but the big part of threat is generated by technical errors, accidents, natural disaster etc. In general, CIP system should be capable to propose two-level package of measures, namely measures aimed at threats diminishing and crisis resolving. The goal of the CIP system is to minimize the risks of ending of operation of CI through building tools of protection (priority for *reliability and resistibility*) as well as to prepare options for quick restoration of CI functionality (priority for *resilience*).

• *Demonstrate added value of CIP system.*

The growing threats from malicious actions against CI require a proactive policy. The CIP system will assess the risks to continuity of functions infrastructure through cooperation of government as well as operators of CEI through establishing close private-public partnership decreasing state expenditures. These functions could be resolved by means of the terrorist treats reaction system. However CIP should cover also other types of targeted actions that include political decisions of other states too (like a decision of Russia to halt energy supply to Ukraine).

• *Use of existing possibilities (institutions and tools)*

Institutional structure which exist today, for example civil protection system, is designed for peaceful time. This system could be used for implementation of a new CIP concept.

[13] Order of Cabinet of Ministers of Ukraine №1337 from 21/12/11. (in Ukrainian). Access: http://zakon4.rada.gov.ua/laws/show/1337-2011-%D0%BF
[14] Order of State Committee on nuclear regulation №163 from 22/11/2010. (in Ukrainian). http://zakon2.rada.gov.ua/laws/show/z1264-10
[15] Requirements for such system reflected in the EU regulation №994/2010 on measures to ensure the security of gas supply, which requires from national governments to develop a Preventive Action Plan and Emergency Plan in the area of gas supply.
[16] Order of Cabinet of Ministers of Ukraine № 809-p from 5/08/15. Access: http://www.kmu.gov.ua/control/uk/cardnpd?docid=248406431

However the focus of the activity should be tuned on other target. The CIP targeted to ensure continuity of functions infrastructure provides, not at protecting of "usual conditions of existence" for citizens and mitigating the outcomes of emergency what supposed to remain the domain of civil protection service.

That target requires the establishment of "preventive action planning" giving special attention not only to build physical protection at all stages of life cycle of CIP (design, location, construction, installation, commissioning, operation and liquidation of consequences) but also to develop interconnectivity of CEI and availability of needed reserves.

These tools of building resilience for some objects are well developed in Ukraine nevertheless it should be formalized in CIP concept through development of "National Preventive Action Plan" as well as "Preventive Action Plan" for CIP operators. In August 2015 this approach was used for the development of "Plan for energy sector functioning in winter period 2015-2016"[15]. Actually this element of CIP system is developed in the physical protection of nuclear facilities and could be adapted to other CI according to provisions of GP.

• *International cooperation*

International experience and support is very important, especially for countries that are limited in resources to develop CIP system on its own. It is important not only through using "best practices", methodology or legislation but also through direct involvement of experts in development of "National Preventive Action Plan". For example, in 2015 the elements of "contingency planning" concerning energy sector of Ukraine was developed by the team of experts from USA, Canada and EU countries as well as "Plan for functioning of Energy Sector of Ukraine in winter period of 2015/2016"[16] and "Plan for achieving of energy sustainability of Ukraine". Plans for separate companies (objects) have been prepared and executed in the same pattern.

Another example of useful international cooperation is conceptual policy on CI and development of framework legislation. The Green Paper on Critical Infrastructure Protection has been created by the National Institute for Strategic Studies of Ukraine with the support of experts from NATO countries.

Hybrid threats: overcoming ambiguity, building resilience
Expert level workshop, September 10th - 11th, 2015
Workshop proceedings publication

Social Resilience in Lithuania: The Lithuanian Riflemen's Union Experience

Dr. Kristijonas Vizbaras,
Brolis Semiconductors, Lithuania

Russian invasion into Ukraine sparked intense emotions in the society of Lithuania. The fact that in modern era independent state borders and international law can be neglected brought back the recent memories of atrocities caused by the very same Russia and Nazi Germany in Lithuania. Despite the fact that Lithuania is both a North Atlantic Treaty Organization (NATO) and a European Union member state, the society did not feel safe. Moreover, the Russian pro-Putin propaganda increasingly spread across all imaginable media channels and started openly addressing ethnic minorities and people living in the periphery with lower income and education level. These facts triggered social resilience in Lithuania, especially among well-educated people, who typically are patriotic and proud of the achievements of independent Lithuania. The phenomenon could be called a special "Lithuanian feeling". A very similar effect was produced by the invasion of the Soviet Union and Nazi Germany into Lithuania during WWII, which lasted until the second Soviet occupation. Teachers, students, officers, engineers, poets and many others joined the ranks of the resistance movement.

Dr. Kristijonas Vizbaras, Brolis Semiconductors, Vilnius

Kristijonas Vizbaras is Co-founder and CTO/Head of epitaxy of Brolis Semiconductors (Vilnius, Lithuania), a high-tech semiconductor technology company and co-founder of Brolis Photonics Solutions Ltd (Larne, United Kingdom), a high-tech company, specializing in advanced laser-based and night vision systems for security and surveilance. His field of expertise encompasses molecular beam epitaxy of III-V semiconductors, with a special focus on arsenides, phosphides and antimonides, where his innovations have resulted in a number of world-record devices, such as room-temperature type-I GaSb lasers down to 3.8 μm, extremely low-resistive tunnel junctions and world-record high-power superluminescent diodes. He has a BSc in EE from the Vilnius University (Lithuania), MSc in Physics from the Royal Institute of Technology (Sweden) and a PhD from Technische Universität München (Germany). Kristijonas has authored and co-authored more than 30 publications in leading scientific technical journals and conference proceedings and has given 8 invited talks in world's leading photonics conferences. Kristijonas has authored and co-authored 3 international patent (pending) applications (1 EP and 2 PCT) while at Brolis. Apart from his professional activities, Kristijonas is a member of the Lithuanian Riflemen's Union, which awarded a Riflemen's Union badge of Excellence (3rd class order).

In 2014, after the Crimea occupation, social resilience in Lithuania gathered into the historic volunteer militia organisation "Lithuanian Riflemen's Union" (LRU). This organisation dates back to the Lithuanian Independence wars in 1919, when volunteers with non-military background decided to join the regular armed forces for the cause of the country through self-financing. It also was very active during the interwar period, when it counted over 60 000 members. It was terminated and disbanded by the Soviets in 1939. Many of those disbanded members were slaughtered by the Soviets, many others joined the armed resistance against the occupants and fought until 1953 and beyond. It is worth noting that several dozens out of those disbanded 60 000 participated in the infamous holocaust and partnered with Nazis putting up the undeserved shadow of shame on the whole organization that we still run today. The LRU was officially re-established in 1989 and its importance peaked during the events of the restoration of Lithuania's independence. Indeed, LRU members actively participated in defending the critical infrastructure (e.g. parliament, TV tower, and so on). Some of them were even killed in action during the bloody events in January and August 1991 in Lithuania. The LRU was officially recognized by the independent Lithuanian state. It was included into the National Defence and Security Law that envisaged its partial subordination to the Lithuanian Ministry of Defence and Chief of Defence. As time went by, the importance of the Union gradually faded, especially after Lithuania's accession to NATO. However, the war in Ukraine put LRU into the spotlight. Its historic significance and legal status made it a preferred organization and the best platform for strong civic defence front.

Today LRU gathers approximately 10 000 members, which are far from the interwar 60 000. However, its growth during 2014 and 2015 was very high. Only in Vilnius, there has been a tenfold increase in active adult (18 – 50 years old) members – from 100 to 1000 in less than a year. In order to keep the new-

Figure 1. Riflemen taking part in weekend tactical training exercises led by professional officers from KASP.

comers satisfied and ensure further growth of the organization, the scopes of LRU activities have been changed and many new ones have been introduced. Today, the main activities are: 1) awareness raising and information war; 2) combat training; 3) counteracting ethnic segregation; 4) cooperation with law enforcement organizations and allies; 5) counteracting anti-governmental activities.

During the 2014 – 2015 period, the LRU was not only the Nordic-Baltic regional role-model volunteer organization promoting civic defence and counteracting indifference, but also the most important organization of this kind. LRU's growth and evolution caught the attention of national and international media. The organization experienced a huge exposure to famous and influential media channels such as Deutsche Welle, radio France international, Deutchlandfunk, the Finnish main TV channel YLE Nyheter, the Swedish main TV channel SVT1 and many others. Articles about LRU circled all over the world in magazines like Newsweek (US), Focus magazine (DE) and Capital magazine (DE), just to name a few. All TV reports and magazine articles contained the message of LRU members to the world that Lithuanians are willing to defend their freedom, they are pride and willing of protecting their European values, Lithuania is not Russia and everyone in the Baltics joins the cause. In such a way, we tried to leave as little as possible space to Russian pro-Putin propaganda that spreads across all over the western world. However, the main achievement of the LRU was the organization of the international conference "Civil Defence in Hybrid Warfare" in Vilnius in 2014. This was a self-organized, self-financed and self-marketed event that attracted more than 400 people in the seated audience and thousands of people watched it live on TV. The guest speakers included The Economist editor and Russia expert Edward Lucas, notable NATO Strategic Communications Centre of Excellence (StratCom) members, defence experts from the European Union (EU) and Ukraine and many others.

In 2015, the above mentioned activities related to awareness raising and counteracting Russian propaganda continued and expanded. In this context, the introduction of intense combat training was of outmost importance. As LRU was well-known in the Lithuanian society, we found it relatively easy to attract very prominent instructors from law enforcement organizations and the Lithuanian Army. They helped establish quality training courses on weapon wielding and full-scale tactical exercises that involved several hundreds people. These courses culminated in joint national rapid reaction force exercises lasting several days. It is worth noting in particular "Lightning Bolt 2015" and NATO Special Operation Forces (SOF) exercises "Flaming Sword 2015" in which LRU took active part for the first time in 25 years. This was useful as LRU practiced the necessary measures that its units would adopt in case of need. The classical activities of counteracting ethnic segregation continued in the form of free-of-charge summer camps for children from different ethnic backgrounds and social conditions. It is necessary to stress here that in spite of Russia's effort to target Lithuania's national minorities in the south-east of the country, this region is one of the most active in providing junior LRU members. This means that LRU's efforts to coounteract the segregation are paying off already.

Another important aim of LRU's activities is the cooperation between LRU and Lithuanian law enforcement organizations. The most highlightning example is the cooperation between Lithuanian Border guards and LRU. It got started in mid-2014 when LRU members joined the weekend patrols of the border guards, doubling the man power and resulting in effective stopping illegal border crossings and smuggling in several cases. However, numbers are only one part of the story, the absence of moral support is the other one. LRU's experience in patrolling with border guards indicates that these servicemen very often feel forgotten by the society, they are misled mainly by Russian and

Figure 2. A Russian GRU officer teaching the pro-Russian group in Lithuania how to use a "Mukha" RPG-18 64 mm grenade launcher in Rudninkai shooting range (NATO territory), belonging to Lithuania's Ministry of Interior in July 11, 2014. 50 km from Vilnius. The insignia on the shoulder is the batman, famous GRU spetsnaz insignia. The uniform – Russian Spetsnaz "Gorka-3".

Lithuanian media propaganda and are not aware of the real importance of the job they are doing. With riflemen joining the service on weekends, these problems were and still are effectively dealt with by the organization. Since most of the riflemen are very well educated and many of them are well-known decision-makers and opinion-shapers nation-wide, very effective education progress has been achieved and huge moral support demonstrated, which will hopefully have a lasting positive effect.

Finally, as an organization uniting people that are patriotic and focused on the cause of national interest, LRU very effectively contributes to counteracting anti-governmental activities and ineffective governmental institutions. A very good example of this is the discovery and elimination of a group of openly pro-Russian and anti-Lithuanian people that had been training in the governmental shooting range (belonging to the Ministry of Internal Affairs) for several years under the corrupt protection of the Ministry of Internal Affairs (MIA) armed forces. The group had not only been training, but had also been trained by Russian Gosudarstvenoje Razvedocnoje Upravlenije (GRU) officers (according to the insignia) and had been utilising a whole set of illegal weapons (see figure 2), such as Mukha Rocket Propelled Grenade (RPG)-18 grenade launchers, automatic-fire rifles and so on. Their battle-dress always was the Russian *spetsnaz*, similar to the "gorka" style, with all the possible add-ons that create an atmosphere of Russian armed force base. According to our calculations, it is possible that in 2013-2014, they provided training on military-grade weapon use to 1000 people. LRU has observed the anti-governmental group's activities by infiltrating them and gathering evidence, which was then delivered to intelligence services with few results. These activities were terminated only when information reached the President and Her Excellence intervened.

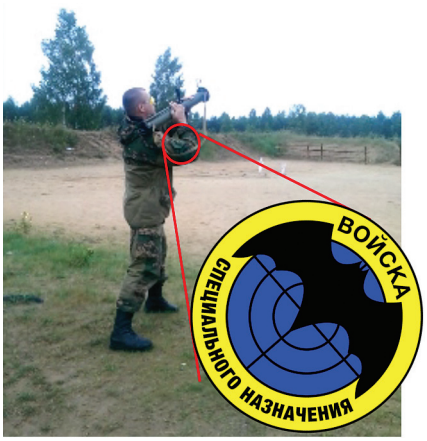

Figure 3. Typical battle-dress of the pro-Russian group active in Lithuania. Uniform: Russian Spetsnaz "Gorka" type.

To summarize, in 2014 LRU reappeared in Lithuania's society by creating a very important self-financed, volunteer-based center of social resilience. It is very active and effective in counteracting Russian propaganda, in preparing people for civic defence, in uniting people of various ethnicities and professions, and in effectively counteracting anti-governmental activities in Lithuania.

NATO Energy Security Centre of Excellence

Šilo g. 5A, LT-10322 Vilnius,
Lithuania
Phone: +370 706 71000
Fax: +370 706 71010
Email: info@enseccoe.org
www.enseccoe.org.

9 772335 797009