WARSAW SECURITY FORUM

2015

Road to

Warsaw Security Forum 2015

5 - 6 November | Warsaw

Road to

Warsaw Security Forum 2015

5 - 6 November | Warsaw

Table of contents

Paweł Soloch
Chief of National Security Bureau

Challenges for the security policy of the Republic of Poland

Road to WARSAW SECURITY FORUM 2015

The world we live in is less and less safe. The uncertainty is growing, the risks are mounting. The most serious threats and challenges since the end of the Cold War have emerged in our environment, and these are not only asymmetric or/and hybrid hazards, but the traditional military aggression as well.

In the East it is imperialistic, revisionist policy of Russia that became the main source of threats. Actually, it is not only the challenge for the Central and Eastern Europe. Aggressive activities of Russian authorities are threatening the very fundaments of the whole European security system, based on the CSCE/OSCE rules, disarmament regimes and multilateral agreements. Russia has been questioning this system at least since 2008, both in its rhetoric and practice, the most vivid example of which is its aggression against Ukraine and illegal annexation of Crimea. All these elements clearly indicate that change in the Russian foreign and security policy is enduring and should be treated as such by NATO and European Union. Russian military expenditures have been growing rapidly, armed forces have been undergoing intensive modernization, vast military operations with offensive scenarios have been exercised, operational capacities have enlarged.

Simultaneously, the southern neighbourhood of Europe is sinking into chaos, generating both terrorist and socioeconomic threats. Arab Spring, welcomed with hope as a chance for promotion of democracy in Middle East and North Africa did not play such a role. In the contrary, the whole area has been affected with acute crisis of state institutions, used by co called Islamic State.

Al-Kaida is still active in the region. In this context, presence of foreign fighters going from Europe to Syria and Iraq and particularly the perspective of their comeback to countries they come from, constitutes a serious challenge.

Another, even more severe problem is the massive inflow of immigrants and refugees from North Africa and Middle East to Europe. The range of this phenomenon is unprecedented and affects not only EU countries, but also countries aspiring to the EU, located on the way from Turkey and the Balkans to Central Europe.

Sustainable anchoring in Euro-Atlantic security structures gives Poland the comfort of common, allied reaction to new challenges.

That does not mean, though, that we should be a passive observer of the situation. Polish security policy must be active.

At the moment Euro-Atlantic structures (NATO, EU and OSCE) are starting strategic reflection on the necessary adjustments of their activities to the changing security environment. In context of these processes Poland will be aiming for preserving the strong position of NATO and UE in the European security architecture and preserving the principles of international law based on the rule of respecting sovereignty and independence of nations and disuse of military power in the foreign relations. Ensuring security by obeying to international law was the main message of the address of Mr Andrzej Duda, the President of the Republic of Poland at the 70th Session of the General Assembly of UN.

The key external pillars of Poland's security remain NATO, UE and partnership with the US. The NATO summit in Warsaw in 2016 should, in our opinion, enhance assurance and adaptation measures adopted in Newport. For Poland the most important question remains strengthening the Eastern flank of NATO by, inter alia, ensuring sustainable presence of allied forces and infrastructure in countries of Central and Eastern Europe. Our task, facing the growing risks, is to care for NATO determination for strengthening its deterrent potential, defense capabilities, as well as its political cohesion and solidarity. On the other hand, works on European Union global strategy on foreign and security policy should lead to strengthening credibility of the Common Security and Defense Policy. EU should also supplement competence of NATO in the area of non-military security, i.a. energy, financial and social security. Poland also firmly supports further tightening of EU-NATO cooperation.
Poland will aim at deepening its cooperation with strategic partners: the US, Western European allies, but also countries from our region. American military presence in the European continent remains the key factor for European security. A good signal in this matter was announcing European Reassurance Initiative by Barrack Obama on 4th June 2014 during his visit to Poland.

The eastern dimension of European security remains a very special challenge. Facing dramatic changes in this area and difficulties in the process of bringing Eastern European countries closer to Euro-Atlantic structures, Poland must undertake more ambitious Eastern policy especially towards Ukraine, Georgia and Moldova. It is necessary to present these countries with an offer which would be meaningful and credible. This includes not only material help (e.g. for Ukraine), but also strengthening presence of

Polish economic entities and Polish culture in Eastern Europe. It is not going to be possible without assistance of the state institutions.

As regards internal dimension of Poland's security policy, the priority is to adopt the comprehensive and integrated approach to the national security, based on the stable, robust financial basis. We need to strengthen the potential of Polish Armed Forces and enhance our modernization and procurement programs (using domestic defense industry potential as well). It is necessary to enlarge mobilization abilities and develop territorial defense. We also need to pay more attention to protection of critical infrastructure and cyber defense.

Strengthening Polish security is nowadays more than in the past decades connected with preserving and strengthening NATO, European Union and a wide system of our bi- and multilateral security and defense cooperation. Nevertheless our own efforts need to be enhanced as well in order to have this task accomplished.

Paweł Soloch

Chief of National Security Bureau

Mr Soloch has been president of the Sobieski Institute think tank. In the years 2005 through 2007 he was deputy minister of interior. On August 7, 2015 President of the Republic of Poland Andrzej Duda appointed him as Head of the National Security Bureau.

JAN PIEKŁO
Director of the PAUCI Foundation

OSCE 'BIS': A New European Security Initiative

Road to WARSAW SECURITY FORUM 2015

Jan Piekło argues that the security architecture in Europe is failing. It is currently based on the legacy of the Helsinki Final Act and the UN Charter which the United States and the EU hoped would preserve peace on the European continent after the end of the cold war. However mutual trust between Russia and the West has deteriorated since the early 1990s starting with differences over the Balkan Wars, the war between Georgia and Russia in 2008, and now the continuing confrontation between Russia and the West over the Russian annexation of Crimea and the invasion of Eastern Ukraine. 'Frozen conflicts' in the post Soviet space have not been resolved despite efforts by the OSCE and others. Countries like Ukraine, Georgia, and Moldova, which have signed Association Agreements with the European Union, now feel exposed, given the weakness of the OSCE and the UN and the failure of Russia, the United Kingdom, and the United States, to respect guarantees they offered to Ukraine in the Budapest memorandum of 1994. Jan Piekło suggests that a new soft security organization, 'OSCE BIS', should be established. This new organization should have Ukraine, Moldova, and Georgia - the signatories of the Association Agreement with the EU - at its core. Other members would be the US, Canada, the EU, and possibly Japan and South Korea, together with those post-Soviet states which can point to a consistent democratic record of government. The absence of Russia in 'OSCE BIS' would reflect the fact that Russia, over the 4 past years, has used the OSCE to serve its own ends and paralyzed OSCE activities when the organization attempts to secure the sovereignty and democratic governance of states in the region. Once Russia establishes its own democratic credentials and withdraws from occupied territories then it would be welcome to join the new organization Piekło says.

FORTY YEARS HELSINKI: A SUCCESS?

This year Europe celebrates the 40th anniversary of the Helsinki Final Act. The Helsinki Declaration was the first act of the Conference on Security and Co-operation in Europe, which took place in the Finnish capital. Thirty-five states, including the USA, Canada, and the European countries except Albania, signed the joint declaration which sought to improve relations

between the Communist bloc and the West. Later, the Helsinki Accords served as a framework for the launch of the Organization for Security and Cooperation in Europe (OSCE), established by the Charter of Paris. The Charter was adopted by a summit meeting of most European governments, the US, Canada and the Soviet Union, in Paris in November 1990, on the basis of the Helsinki Act. It was further amended in the 1999 Charter for European Security. Both these documents form the basis for the Organization for Security and Cooperation in Europe. In the next decades this framework, contributed a wide range of diplomatic instruments for solving potential crises and kept the security balance in Europe. The OSCE and the United Nations (UN) guaranteed the inviolability of the frontiers and the territorial integrity of states.

After the dissolution of the Soviet Union the Russian Federation was declared the successor state of the USSR on the grounds that it contained 51% of the population of the USSR and 77% of its territory. As a consequence, Russia got the USSR's permanent seat on the UN Security Council.

This was accepted by the other former republics of the Soviet Union. Ukraine, as a new independent state, agreed to give up its nuclear stockpile – the world's third largest. The Budapest Memorandum, signed in December 1994, offered security assurances concerning the threat or the use of force against the territorial integrity 5 and political independence of Ukraine, as well as that of Belarus and Kazakhstan. The Memorandum was signed by three nuclear powers: the Russian Federation, the United States of America, and the United Kingdom.

HOW RUSSIA UNDERMINED THE SPIRIT OF HELSINKI

After the dissolution of Soviet Union, the Russian Federation - as its legal successor – fuelled local, mostly ethnic, conflicts in its closer neighborhood and thereby managed to construct "frozen conflict" zones – which worked as a leverage for securing the Kremlin's geopolitical interests. These zones were separatist Transnistria in Moldova, Abkhazia and South Ossetia in Georgia, and Nagorno-Karabakh, which, after the Azeri-Armenian war, became a de facto part of Armenian territory. The fragile security architecture, constructed in Europe some years earlier, was challenged and the work of Pan-European security organizations (and various ad hoc contact groups set up to solve regional problems) became less and less effective.

The Yugoslav crisis, which led to ten years of Balkan wars, posed a new challenge for the existing European and global security institutions, and exposed the weakness of the UN peace keeping mandate and conflict prevention mechanisms.

When the Pan-European cooperative security structures were challenged and then invalidated by the Yugoslav wars, the OSCE realized that its role in conflict prevention lay more in the normative and soft security dimension. In 1992, the OSCE created the Conflict Prevention Centre (CPC) to serve as a focal point in European early warning and dispute settlement. However, with minor exceptions, the CPC was bypassed during the explosion of deadly violence in the Balkans. States with a vital stake in the unfolding conflict apparently preferred to pursue their policies through the European Union, the UN, and, ultimately, through international ad hoc contact groups". [1]

NATO's military intervention through air strikes and the ground deployment of soldiers finally managed to end the Balkan war. It is worth stressing that in this case it was military action which finally brought a diplomatic and political solution to the conflict. Russia, which supported the Serbs from the very beginning, considered the NATO actions and Western peace settlement (especially the recognition of Kosovo's independence) as a geopolitical defeat.

[1]Fred Tanner, "Conflict prevention and conflict resolution: limits of multilateralism," International Review of the Red Cross, No. 839, September 30, 2000. (Fred Tanner is Deputy Director of the Geneva Centre for Security Policy).

THE OSCE AND THE RUSSIAN AGGRESSION IN UKRAINE

Consequently Moscow developed a plan for revenge. The first clear signal of Russia's openly aggressive intent came with the war in Georgia in 2008. Moscow blamed Mikheil Saakashvili and the Georgian side for provoking the conflict and the West quite easily accepted the Russian version of events. Partly because of this Saakashvili first lost his popularity, and then the election at home. The real crisis came in 2014 with the Russian annexation of Crimea and the military invasion in Eastern Ukraine. It was Moscow's reaction to the Euromaidan Revolution in Ukraine and to the decision of the new, democratic government in Kyiv to sign an Association Agreement (AA) with EU. Through this act of aggression and violation of the territorial integrity of Ukraine, Russia invalidated the whole fragile European

security architecture, based on the Helsinki Accords. Moscow broke also the UN Charter. The democratic world community reacted to this development by using the existing international diplomatic instruments, which the OSCE, the UN, and the Council of Europe offered. New ad hoc initiatives were also set up such as the Minsk contact group and the Normandy and Geneva formats to negotiate the conditions of the successive ceasefires.

Russia, as a signatory and co-founder of global and Pan-European institutions, used its membership to manipulate and blame the West, the EU, NATO and Ukraine, for provoking this deadly confrontation. The situation created a deadlock, which blocked the chances of solving the most serious crisis on the European continent since the Balkan wars. The already invented security instruments at the disposal of the West proved to be ineffective and ill-suited for dealing with the former partner of the West, who had unilaterally changed the rules of the geopolitical game. Ukraine, Moldova, and Georgia, the three Eastern Partnership (EaP) countries which decided to sign Association Agreements with the EU, are now left without any security and political guarantees.

In the case of Ukraine, Kyiv found it had lost the guarantees of territorial integrity which had been included in the Budapest Memorandum. Since the Bucharest Summit in 2008 the subject of closer links between NATO, Ukraine, and Georgia, came off the agenda. After the Euromaidan Revolution, which made many victims among the activists who fought for "European values" in Ukraine, the EU and the transatlantic community, apparently, left their partners without any constructive support. While it is fighting 'separatists', who are backed, manned, and financed by Russia, Kyiv is deprived of western weapons support, for which it has been asking for a long time. At the same time the delivery of French Mistral helicopter carriers to Russia is only "temporarily suspended". With permission of the EU, also the German firm Daimler may breach sanctions and help the Russians to develop modern military vehicles.

With the ongoing war on the European continent about 1000 km from the EU's Eastern border and the aggressive policy of Putin's regime, the West found itself in a situation where its basic credibility is at stake. Russia's destabilization efforts can invalidate the Eastern Partnership and bring these countries back under the control of the Kremlin. This will jeopardize the EU as a successful political project. The result will be a new kind of Yalta division of the world.

Russia through blocking and manipulating the existing global and Pan-European security organizations, is preventing that they can be used for finding a solution to the growing confrontation. Therefore, the transatlantic community should consider the establishment of a new security institution which would be able to offer, for the moment, soft guarantees to the countries which have signed Association Agreements with EU.

Some similar initiatives already took place before and after the Orange Revolution (2004- 2005) in Ukraine:

• GUAM was a established in 2001 as an Organization for Democracy and Economic Development . It was a regional intergovernmental organization of four post- Soviet states: Georgia, Ukraine, Azerbaijan, and Moldova. Turkey and Latvia had observer status.

• The Community of Democratic Choice was an intergovernmental organization, established in 2005. Founding members were Estonia, Lithuania, Latvia, Georgia, Ukraine, Macedonia, Moldova, Romania, and Slovenia. Azerbaijan, Bulgaria, the Czech Republic, Poland, Hungary, the US, the EU, and the OSCE had observer status.

• Black Sea Synergy, established in 2006. This was an EU initiative, proposed by Romania. The members were Georgia, Azerbaijan, Armenia, Moldova, Ukraine, and Romania. Bulgaria and Turkey had observer status. Russia, in spite of being invited, showed a lack of interest in this initiative.

These numerous attempts to build up cooperation structures show that even before launching the Eastern Partnership the countries of the region were interested in setting up multilateral networks to protect their geopolitical interests and counterbalance Russian influence in the Black Sea basin. Unfortunately, most of these initiatives are now dead.

The only successful and consistent initiative was the Eastern Partnership, inaugurated in 2009, which was proposed by Poland and Sweden. The EU project targeted Ukraine, Belarus, Moldova, Georgia, Belarus, Armenia, and Azerbaijan. Its aim was to improve trade relations with the EU and bring these countries closer to the EU through offering them AA's. Brussels managed to sign an AA with Ukraine, Moldova and Georgia (However, Armenia, after completing the nego-

tiations, decided to step away from the AA and join the Kremlin's Eurasian Union). When the EaP turned out to be successful Russia reacted with military force. It attacked Ukraine, breaking its international commitments.

In order to save its own credibility and the EaP initiative, the Western community should offer its Eastern partners some kind of soft security guarantees, based on the Helsinki accords and the UN charter principles which address in the first place the issue of territorial integrity and sovereignty.

THE NECESSITY OF 'OSCE BIS'

This initiative could adopt 'OSCE BIS' as a working title, stressing that it is based on the Helsinki Final Act and the Paris Charter. This initiative should be addressed to:

- Ukraine, Moldova, and Georgia, which are signatories to the Association Agreements with the EU and would, therefore, receive a special status
- Turkey and those Balkan countries which have yet to join the EU, would be members
- Belarus, Armenia, Azerbaijan – on the condition that they improve their democracy Record
- Central Asia countries – on the condition they improve their democracy record
- Russia could be accepted after meeting democratic criteria, and on the condition that it invalidates the annexation of Ukrainian and Georgian territories and withdraws its troops from occupied territories

Special recommendation:
The construction of such a new intergovernmental organization ('OSCE BIS') should include a strong civil society component, based on the already existing Eastern Partnership Civil Society Forum, which should have the right of membership.

The Western side should be represented by the EU, the US, Canada, Norway, Switzerland, and, possibly, also Australia, Japan, and South Korea. The new organization should also be open to new members from North Africa (criteria: democracy record). The name and further legal and structural details can be discussed later after agreeing on the principles given in this discussion paper.

The process of launching a new international organization might be a long and difficult one, but the dynamic of developments in Eu-

rope and the European neighborhood - including the threat posed by Russia and ISIS - requires a fundamentally new approach to these challenges. Unfortunately, Europe failed to learn much from the Balkan conflict.

A well coordinated campaign to publicize this new security architecture concept might persuade aggressive parties, such as Russia, to negotiate, in order to preserve the status quo in the existing security architecture. If Russia does not do so, it risks becoming marginalized, being reduced to a so-called "rogue state." This scenario is definitely not an option Moscow wants. The West should play on Russia's weaknesses.

It is evident that hard security should continue to be provided by NATO. Jean-Claude Juncker's recent initiative concerning the creation of an EU army seems to be counterproductive in the current situation. The EU desperately needs to strengthen the transatlantic relationship and a further rapprochement between the old continent and the US could be the only long-term option for reversing the existing negative security trends. This will take time and it needs a political will on both sides, as well as a consensus among the EU member states.

APPENDIX:

As concerns the "Memorandum on Security Assurances in Connection with Ukraine's Accession to the Treaty on the Non-Proliferation of Nuclear Weapons, signed on 5 December 1994 by the Presidents of Ukraine, the Russian Federation and the United States of America, and the Prime Minister of the United Kingdom of Great Britain and Northern Ireland," which is known as the "Budapest Memorandum," Irina Paliashvili wrote: "The technical and legal intricacies of its language can be discussed ad nauseam, but nothing can change its bottomline: the three signatories – the US, the UK and Russia - confirm and reaffirm 'their commitment to Ukraine in accordance with the principles of the Final Act of the Conference on Security and Cooperation in Europe, to respect the independence and sovereignty and the existing borders of Ukraine'."

"There is no doubt that Ukraine has delivered on its commitments under the Budapest Memorandum

promptly, fully and in a good faith. The two guarantors, the US and the UK, are in a possession of overwhelming and undeniable evidence of continuing violation by Russia of "sovereignty and the existing borders of Ukraine", first by occupying and annexing Crimea, and then by invading and waging war in Eastern Ukraine."

Irina Paliashvili "The Budapest Memorandum revisited," Kyiv Post, February 6, 2015.

"The OSCE is allowed to operate at only two checkpoints on the vast Ukrainian-Russian border. Yet from these two checkpoints alone, monitors note hundreds of individuals in military-style dress freely crossing the border every week. The separatists have a larger fighting force, with more weaponry, than some European countries. Meanwhile, Russia is reportedly preparing to deliver its 12th resupply convoy to separatists in Ukrainian territory at the end of the month. If the past eleven deliveries are any indication, Russia will deny international monitors or Ukrainian authorities the ability to fully inspect the convoys. If Russia is indeed sending humanitarian aid, what does it have to hide? ... The current situation is dangerous. It is dangerous because separatists continue to harass, threaten, and intimidate the impartial monitors deployed by the OSCE – monitors who serve on behalf of the international community. According to a January 14th OSCE report, the Special Monitoring Mission, or SMM, was stopped at a separatist checkpoint in Oktyabr by a hostile separatist commander who ordered the team's car searched and said the monitors would be shot if a camera was found, even though cameras are a basic tool of documentation work. Separatist guards kept their guns pointed at the monitors during the exchange, the monitors said, even though the team posed no threat and, mercifully, had no camera."

Remarks by Ambassador Samantha Power, U.S. Permanent Representative to the United Nations, at a Security Council Briefing on Ukraine, January 21, 2015.

"As this is the last scheduled PC of 2014, it's a time to take stock. Next year, as we all know, marks the fortieth anniversary of the Helsinki Final Act. That Act, the founding document of this Organization, enshrined ten fundamental principles designed to guide the relationships among participating States. Those ten principles – referred to as the Decalogue – are the carefully negotiated and agreed foundation of this Organization and provide the means for ensuring comprehensive security for the States represented around this table, and most importantly, for our citizens."

"Over the past eight months, through its actions in and around Ukraine, the Russian Federation

has failed to uphold the principles in the Decalogue. Russia has violated Ukraine's sovereignty and territorial integrity and intervened in Ukraine's internal affairs. Russia has undermined efforts to resolve the crisis peacefully through the Minsk Protocol and agreements, to which Russia is a signatory, through continued military, political, and financial support of the armed separatists operating in eastern Ukraine. De-facto authorities in Crimea have abused the human rights and fundamental freedoms of the people living there, and Russia has actively supported pro-Russia separatists as they abused the human rights of Ukrainians. Russia has made a mockery of the fundamental principle of self-determination through the so-called "referendum" held in Crimea. Russia's actions have undermined cooperation among States."

"The consequences of Russia's actions are suffered every day by those killed and wounded in the fighting in Ukraine's Donbas region. They are felt by the people in eastern Ukraine struggling to find food and shelter in conflict areas, as highlighted recently by the United Nations. They are felt by the people of Crimea forced to live under an occupying power."

Ongoing Violations of OSCE Principles and Commitments by the Russian Federation and the Situation in Ukraine.

As delivered by Ambassador Daniel B. Baer to the Permanent Council, Vienna, December 18, 2014.

"The international community is united in condemning the violence that has led to so much needless suffering in Ukraine, but the violence continues. Regrettably, Russia continues to supply new weapons and increase support for armed separatists. In doing so, it fails to meet its international and OSCE obligations and to live up to an agreement that it actually negotiated and signed. The result is damage to its credibility, and its own citizens wind up paying a steep economic and human price, including the price of hundreds of Russian soldiers who fight and die in a country where they had and have no right to be.

My friends, more broadly, the crisis that we have experienced in Europe this past year is not the fault of the international system. It stems from the unwillingness of individual actors to abide by the rules and the principles of that system. When rules are broken, they need to be enforced, not rewritten. Despite numerous violations of Helsinki this year, the timeless wisdom of the final act – that sustainable security can only be achieved when fundamental freedoms and human rights are protected – has been reaffirmed. To build a more secure

OSCE area, we need to acknowledge the serious failure of some member states to live up to their responsibilities, and these failures affect us all.

In closing, I thank President Burkhalter once again for his stewardship, the people of Switzerland for their hospitality, and we look forward to working with Prime Minister Vucic and Foreign Minister Dacic during Serbia's chairmanship next year. And you will be sure that you will have our support as we celebrate the 40th anniversary of the Helsinki Final Act. Thank you."

Remarks by Secretary of State John Kerry at OSCE Ministerial Plenary Session, December 4, 2014.

Jan Piekło

Director
PAUCI Foundation

Since May 2005 director of PAUCI (Poland America Ukraine Cooperation Initiative then transformed to the Polish-Ukrainian Cooperation Foundation) which manages the trans-border projects with Ukraine, Moldova, Georgia and Armenia. Till May 2005 he worked as a program director for ZNAK Foundation in Krakow, supervising different educational/journalism programs. As a journalist, he covered the Romanian Revolution and war in the former Yugoslavia.

Derek Chollet
Counselor and senior advisor for security and defense policy at the German Marshall Fund of the United States

After Ukraine, NATO's Chance for a New Normal

Road to WARSAW SECURITY FORUM 2015

Can Defence Secretary Ash Carter and European leaders turn NATO's historic Ukraine response into a new future for the alliance?

Listening to politicians and pundits on both sides of the Atlantic, it would be easy to conclude that U.S.-European relations are suffering a major crisis. There is a surplus of breathless talk about frayed alliances, a vacuum of leadership, and European jitters about American withdrawal. Yet the reality is better than it seems — and at the same time, it is also more complicated.

While some see the Ukraine crisis and the threat of a revanchist Russia as exposing fundamental weaknesses in the transatlantic security alliance,NATO's response has revealed more of the alliance's strengths than its shortcomings. It has also been a reminder of NATO's indispensability. That will be a key message next week during Secretary of Defence Ashton Carter's first major trip to Europe at the Pentagon's helm, where he will make important stops in Germany, Estonia and Brussels for his first NATO meeting of defence ministers. What's to be seen is if NATO can turn the temporary attention of the Ukraine crisis into a permanent evolution of the alliance. Has NATO found a new norm?

Let's start with the good news. The past year has seen the most significant shift in the transatlantic security relationship since NATO's entry into Afghanistan after 9/11. First, from the moment the Ukraine crisis erupted, U.S. and allied forces have maintained a persistent land, air and sea presence in NATO's Eastern front-line states. None of this existed before. For the United States, this includes a rotational presence of troops in the Baltics and Poland. Now the discussion is whether to preposition heavy armor and equipment in those locations—a possibility that President Barack Obama's $1 billion "European Reassurance Initiative" put on the table last year—and whether such deployments should be permanent.

Second, U.S. and European leaders have pursued an aggressive sequence of major military exercises. This year has seen the most significant American military training in Europe since the end of the Cold War. Right now approximately 15,000 troops from 19 NATO countries are participating in "Allied Shield," an exercise to enhance interoperability, readiness, and re-

sponsiveness. This builds NATO's capabilities to work and fight together, and sends a clear message to Russia that the alliance's commitment to collective defence remains robust.

Third, the Ukraine crisis has jump-started the NATO discussion about military capabilities. For years, U.S. defence leaders have been hectoring their NATO partners to increase spending, a message Carter will certainly echo again. But too often, this was perceived as more of a theoretical debate against an ill-defined foe. Now, the wide acknowledgement of Russia's military threat has caused many NATO partners, particularly countries like Germany, Poland, and the Baltics, to step up and invest more in defence.

Finally, the past year has seen a shift in the debate about the purpose of NATO itself. While the concern now is whether NATO will maintain the will to meet these new challenges, it was not so long ago, just before the Ukraine crisis, that some wondered if NATO was still relevant at all. In the early days of planning for last year's NATO Summit in Wales, those of us in the U.S. government worried that the Summit would be dominated by existential questions like whether we still needed NATO and what the Alliance's purpose would be after its withdrawal from Afghanistan. Yet the crisis in Ukraine (as well as the exploding crisis to Europe's south and the insecurity emanating from North Africa) clearly demonstrated NATO's enduring relevance.

Vladimir Putin did more to make NATO relevant than any of us in government at the time could have wished.

But therein is the challenge. NATO's responses over the last year have been reactive and by definition (when measured by budgets) temporary. So the question NATO leaders must answer — and that Carter should push at next week's ministerial meeting – is to decide how to transition these steps into a sustainable, fully-resourced "new normal."

And this is where things get complicated.

Although U.S. officials and pundits often assert it is all about us Americans—and there remain plenty of policy issues for Washington to sort out—the main complication is the divisions within Europe. It is neither America's military posture nor its commitment to Europe.

At the most abstract level, the biggest divide lies between Europe's East and South.

For good reason, the Baltics and Poland see Russia as the predomi-

nant threat, something that Carter will hear in spades when he meets with his three Baltic counterparts gathered in Estonia. But they compete for attention with those on NATO's southern tier who are more worried about the refugee crisis, which is the worst in Europe since World War II.

More specifically, the top European contributors to NATO's defence are on a different strategic page. The UK is consumed by its own existential question about its future in the EU, as well as a defence budget that is being drastically cut. France has emerged as one of the most reliable and steadfast defence partners but is intensely focused on Africa's Sahel, where it has over 3,000 troops deployed. Italy also worries mostly about the crisis to its South, especially Libya, where it has seriously talked about inserting a peacekeeping force. Poland is seized with the threat from Russia, as its 18 percent increase in defence spending this year shows.

And Germany, which has asserted itself as Europe's leader on Ukraine, still wrestles with the role of its military in projecting German influence. As I have argued earlier in Defence One, German Defence Minister Ursula von der Leyen is one of Europe's most interesting (and active) defence leaders, and has emerged as one of Carter's closest counterparts. Carter will be the first U.S. defence secretary to visit Berlin in nearly a decade, where he will deliver the main policy speech of his trip.

These divisions—between East and South, about competing priorities and interests—create a strategic cacophony that raises questions about Europe's ability to sustain its end of the bargain in providing for a shared defence. For all the Alliance has accomplished in the past year to show its resolve, and for all the earnest rhetoric about common purpose, how these tensions are managed will define the transatlantic relationship. As Henry Kissinger put it nearly four decades ago, the alliance must be held together by more than "the highest common platitude."

Derek Chollet

Counselor and senior advisor for security and defence policy at the GMFUS

Derek Chollet is a Defense One contributor. He is also counselor and senior advisor for security and defense policy at the German Marshall Fund of the United States. During the Obama administra-tion Chollet served most recently as assistant secretary of defense for interna-tional security affairs and in positions at the White House and State Department.

The Alliance for Innovation
and Infrastructure

Is Europe Truly Unified?

Road to WARSAW SECURITY FORUM 2015

The European Union (EU) was created with the intention of increasing cooperation among European States within a variety of sectors to achieve mutual growth. Since its inception, additional treaties and regulations have been implemented to expand security, trade, and social policies. However, the extent of this unity is brought into question when analyzing the energy markets of Europe.

In the last decade, the European Commission has repeatedly called for a ten percent electrical interconnection among EU members. This plan is part of the Energy Union concept; a comprehensive internal market for Europe meant to stabilize energy supply, reduce costs, and safeguard the environment.

Although brilliant in theory, one main criticism of the Energy Union is that it is yet to materialize. At least in terms of energy, the EU is more talk than action. The ten percent goal has been reiterated over the course of thirteen years without coming to fruition. Several factors contribute to the delay, including the lack of an effective management structure, misaligned goals, political history, and differences in national interests. Apart from a volatile supply and high-energy costs faced by consumers, a lack of such a Union has made much of Europe reliant on Russian energy. This has placed Europe in a compromising position politically and economically as well.

The EU has placed intense focus on fighting climate change in the past decade, taking the lead in the global charge toward renewable energy and making the shift to green energy a primary goal. Some countries grant large subsidies to the renewable sector, disregarding more efficient resources. The implications of this focus have been higher costs and a volatile energy supply; a contradiction of the two main goals for the Energy Union. In the Energy Union plan, climate policy and renewable energy simultaneously take the forefront, while renewable energy is also a primary method of reaching the goal of climate policy. This sporadic agenda pulls Europe in several different directions, which in turn leads to the lack of progress being made on the energy front.

Misaligned priorities among EU members are another obstacle to interconnecting the European energy grid. Certain EU member States have not made this plan a priority and chosen instead to allocate crucial resources to develop basic infrastructure. In some cases, countries with lower technological capabilities than their more advanced partners find it in their interest to remain disconnected. For

example, Poland is disproportionately powered by inefficient coal-fired power plants. The Energy Union plan would see Poland reducing its coal output to rely on more technologically advanced forms power generation. For the Polish people, this may have positive outcomes such as lower energy costs and increased efficiency, but that must be weighed against the loss of jobs at the power plants and in coal related industries. Ultimately, the EU seeks to decarbonize its entire economy and energy practices. This would permanently strip Poland of its coal industry, something the Polish may want to delay. Such issues stand in the way of the overarching goal of uniting an internal market.

Furthermore, the apparent reluctance to collaborate can sometimes be traced back to events in common European history. Various political disputes between countries have lead to a deterioration of trust between certain European States. Germany and Poland stand out as a primary example. Over the course of history, land disputes and differences in political and cultural ideologies have divided these bordering States. As a result of this, the relationship between the two countries is constantly over-shadowed by the specter of the past.

When taken together an overarching issue obstructing the Energy Union appears to be a lack of an effective management structure and a basic blueprint to carry out the project. As a result of this, resources are allocated inefficiently and States are not held responsible or accountable for their lack of cooperation thus leading to a very slow and fractured process.

Taking the above-mentioned matters into consideration, six policy recommendations are encouraged to help guide the creation of a successful energy union:
These recommendations include, but are not limited to the following:

1. The creation of a dedicated EU institution to oversee the European Energy Union project

2. Increased cross-border financing for energy infrastructure

3. Mandatory enforcement of integration deadlines

4. Utilization of Europe's geographical layout to maximize production of renewable energy

5. The creation of regional grids

6. The acknowledgment and

usage of natural gas as a viable source of energy

An Energy Union within the EU has many challenges ahead of it, namely the 28 individual members that make up the Union. An undeniable hindrance to achieving the plan is the call for sweeping policies at the continental level that can at times contradict the policies of member States. It is pertinent to note the issues being raised regarding a potential Energy Union are of the same caliber as those first raised regarding the formation of the EU itself. The Energy Union will succeed, but only if the European States realize the importance of such a fundamental link.

The Alliance for Innovation and Infrastructure (Aii) recently complied a report on the European Energy Union titled "An Energy (Dis)Union: A Critique of the European Internal Market." The report analyzes issues such as historical implications, contemporary economics, and politics, which impact the creation of a European Energy Union. This document serves as a preview outlining several of the major issues raised in the report and the policy recommendations within it. More information regarding the Energy Union, its importance, and a discussion of the recommendations will be available in the upcoming report.

The Alliance for Innovation and Infrastructure

Aii is a U.S. based nonprofit committed to promoting innovative and effective strategies to address a variety of issues currently faced by the energy and transportation industries.

Jagello 2000

Hybrid Warfare: A New Phenomenon in Europe's Security Environment

Road to WARSAW SECURITY FORUM 2015

1. Hybrid warfare as a concept

The war in Clausewitz's concept is seen as a continuation of the policy of the state by violent means, which are used to force the opponent to execute our will. The primary role in this concept is played by the use of armed violence in its symmetrical or asymmetrical form. To this end all the resources of society are used as later elaborated in the concept of total war. Although hybrid warfare serves the same purpose, namely the achievement of political goals, which can be very diverse, it differs from war in Clausewitz's concept (further referred to as 'classic war') in many different characteristics.

Expert debate about hybrid warfare began in foreign literature long before the Russian invasion of Ukraine. In our opinion, this debate's weakness consists in the fact that the available definitions do not set explicit demarcation criteria for distinguishing between classical and hybrid warfare. If we want to differentiate between hybrid warfare and classic war, the main demarcation criterion, in our judgment is the use of the means that are primarily used to achieve the objectives of war. In hybrid warfare, it is important that non-military means of subversive nature play the leading role. Ideally, an attacking state need not make explicit use of military force. The aim of the attacker is to control the minds of the political leadership and the population of the attacked state through propaganda (psychological operations), deceptive campaigns and intimidation by terror. If military force is used, it is used in secret. Use of demarcation criteria, prioritising non-military tools of subversion and conducting secret warfare, these aspects clearly distinguish hybrid warfare from other types of war.

1.1 Working definition of hybrid warfare

Hybrid warfare is an armed conflict conducted by a combination of non-military and military means and aiming with their synergistic effect to compel the enemy to take such steps that he would not do of his own accord. At least one side of the conflict is the state. The main role in achieving the objectives of war is played by non-military means such as psychological operations and propaganda, economic sanctions, embargoes, criminal activities, terrorist activities, and other subversive activities of a similar nature. The attacker's military operations are conducted in secret by irregular forces combining symmetric and asymmetric methods of combat operations against the whole society and, in particular, against its political structures, state authorities and local govern-

ment, the state economy, the morale of the population and against the armed forces.

2. Use of elements of hybrid warfare against Georgia and Ukraine

2.1 Georgia 2008

The Russia-Georgia armed conflict in the summer of 2008 broke out at the time of the Beijing Olympics and aroused deep concern in the international community. According to some experts, it was the first armed confrontation between the East and the West after the end of the Cold War. The main aim of Russia was to retain its influence through military operations, to recognise the independence of the regions concerned, and to maintain a significant military presence in those territories. Last but not least, Russia 'buried' the chances of Georgia to achieve NATO membership in the near future, which Georgia has sought since 2002.

In this case, it was not a hybrid warfare within the meaning of the above-proposed definition. It was a war according to the classical definition, in which Russia openly intervened with militarily force and used some elements of hybrid warfare to prepare and support the conduct of combat operations.

The policy goals of the operation were primarily achieved by military force whereas elements of hybrid warfare (economic sanctions and embargoes, information war, war in cyberspace) played more of a supporting role.

Both sides of the armed conflict waged an intensive information war, making it difficult to separate facts from intentionally disseminated disinformation. This information war was dominated by three main themes:

1. Georgia and especially President Saakashvili were aggressors.

2.Russia was forced to intervene to defend its citizens and to prevent a humanitarian catastrophe (defensive purpose);

3 . The West has no legitimate reason for criticizing Russia because Russia simply does what the West did in Kosovo in 1999.

Parallel to the information war against Georgia, cyber war also took place. A total of 38 Georgian websites were attacked, including the website of the Georgian president, Ministry of Foreign Affairs,

National Bank, Parliament, and Supreme Court. These attacks were centrally managed and coordinated.

It is difficult to evaluate the performance of the Russian armed forces, as it is still not entirely clear whether it was a pre-planned and carefully prepared military operation, or whether it was on both sides an unexpected war, for which neither of the conflicting parties were prepared. However, the rapidity of the deployment of Russian military forces in the mountainous terrain, the early opening of a second front in Abkhazia, Russian espionage activities in the region, military provocations on the eve of war, the downing of a Georgian unmanned aircraft and, last but not least, the Russian military exercises in the region ('Caucasus 2008') demonstrate the readiness of Russia to escalate the conflict. The conflict nevertheless revealed many Russian shortcomings, particularly weaknesses in the coordination of ground, naval and air forces. According to available sources, an important role in military operations was played by airborne units and special forces. The reforms announced by the Russian president immediately after the war reflect the intention to improve Russia's ability to effectively lead the campaign by employing modern technologies and operating procedures.

2.2 Ukraine 2014–2015

Russia used and is still using against Ukraine a wide range of military (asymmetric and symmetric), economic, propagandistic, diplomatic and perhaps even cyber means of combat.

The activity of Russian diplomacy, of course, cannot be summed in a text of this scope and purpose, but in brief, we can say that Russia is seeking to weaken Kiev at forums of international organisations, in particular by promoting the federalisation of Ukraine. Concerning the economic means, Moscow manipulates the price of imported Russian natural gas and adopts restrictive non-tariff measures on Ukrainian food products. For the Ukrainian economy, the most severe sanction is a ban on the use of Russian air space by Ukrainian airlines.

Russia uses the so-called 'new propaganda' that does not seek to persuade the recipient, but to obfuscate what is truth and what the recipient can trust. To enlist support for the war in the Russian population it uses a broad variety of media channels, particularly state television, which in its coverage of Ukraine can significantly influence the local public opinion. These include Russia Today, Voice of Russia, Sputnik, press agency ITAR-TASS and the agency RIA Novosti. It is also worth mentioning that mul-

tiple sources have confirmed the existence of an army of trolls paid by the government. These are Internet bloggers and debaters who post views preferred by the Russian government to domestic and foreign websites.

Concerning the cyberspace area, several attacks against the Ukrainian government websites and systems have been recorded (e.g. the Ukrainian electoral counting electronic system, the Ukrainian transport network, and attacks on websites of volunteer battalions). However, it is not possible to determine with certainty whether it has been the work of the Russian forces. It is also necessary to emphasise that all cyber-attacks are only the tip of the iceberg. The extent of Russian cyber-attacks using malware or spyware can never be determined with certainty unless Russia discloses this information voluntarily (or if it is leaked).

In the military dimension, Russia and the separatists are able to deploy a wide spectrum of units in the conflict. According to the US Department of Defense, in November 2014 Russia had 7,000 regular troops in Ukraine (excluding the Crimea). To this day, it is alleged that more than 40,000 Russian troops have been rotated in Ukraine. Russia and Russian organisations actively support the separatists (with logistics, material and personnel), who are a combination of the local population, Russian citizens and, occasionally, citizens of many other countries. Without extensive logistical support from the outside, it is impossible for the separatists to conduct combat operations to the extent that we see in eastern Ukraine. Russia is the only country in the region that has the capacity and motivation.

If we apply the working definition in the introduction, then we can speak of hybrid warfare in particular to describe the Russian occupation of the Crimea and Russian operations until the summer of 2014.

Evaluation of the conflict since the summer of 2014 is not so clear-cut. Since summer 2014, it is quite obvious that regular Russian troops operate in eastern Ukraine and if necessary (e.g. imminent defeat of the separatists) even entire organic military units can be used. Denying this direct participation of the Russian military belongs to the hybrid warfare tools. On the other hand, the direct military intervention of Russia suggests that hybrid warfare has reached its limits.

3. Is this a new approach?

The bedrock of the hybrid warfare concept is that of subversion, which comprises four main stages:

1. demoralisation of the target society,

2. destabilisation of the target society,

3. precipitation of a crisis in the target society,

4. seizing control of the target society by internal forces acting in concert with the attacker.

This is an old Soviet (Marxist-Leninist) concept, applied towards the West by the USSR throughout its existence. Attacks on the adversary's political authorities, propaganda, fomenting unrest, creating 'people's republics', these are well-known components under the cloak of the new hybrid warfare. Modern information technologies allow multiplication of the effect that brings a new quality and dangerous nature of this phenomenon.

4. Potential of hybrid warfare

Hybrid warfare in the media space is considered extremely dangerous.

The proponents of this view usually refer to the Russian general Gerasimov, who claims that hybrid war can disrupt even a well-governed and prosperous state. This optimism (or pessimism, depending on one's perspective) is difficult to sustain in the light of the current empirical evidence. In a security analysis of this phenomenon, it is important neither to underestimate nor to overestimate its possibilities. The main problem for the defender is to identify the moment when he is the target of a hybrid attack.

Therefore, defence against hybrid warfare depends in the first line on intelligence services and in the second line on an authentic civil society.

To wage a hybrid war aiming to achieve political goals, a number of specific necessary – however not sufficient – conditions must be met. Only their right configuration generates a suitable battlefield for hybrid warfare.

Empirical evidence to date indicates that these are at least the following necessary but not sufficient conditions in isolation:

1. the attacked country has been mismanaged in the long term and it does not fulfil its basic functions,

2. its population is divided along several dividing lines,

3. the potential attacker holds a certain attraction for a part of the attacked-country population and can therefore use soft-power instruments,

4. the attacked country borders the attacker and is unable to effectively control its borders,

5. the attacked country has no dependable allies, and

6. the attacker has a certain degree of credibility in the international community, which allows him to influence the international community with his version of events.

Even in the case of Ukraine, which is in the post-communist milieu the prototype of a poorly governed state, managed like a company that lays golden eggs for oligarchs, the hybrid warfare succeeded only in the first stage in the Crimea.

However, by the second stage, when Russia, encouraged by its success in the Crimea, tried to split Ukraine along the Odessa–Kharkov line, this concept fatally failed and the defeat of Russian irregular forces fighting in secret until then in the east of Ukraine had to be prevented by an open intervention of Russian regular forces in the summer 2014. This intervention continues till today, producing negative political, economic and military consequences Russia.

If we think about further potential of hybrid warfare used against the West and the countries close to it, we must take into account that Russia has lost the element of surprise. Potential targets of this type of warfare, which in our region means primarily the Baltic States and indirectly NATO, would now be less shocked than in 2014. This is relevant also to the other countries of the West. Whether this conclusion applies to Belarus and the Central Asian countries is a question, however. Some steps taken by Belarus indicate that Lukashenko is aware of these risks.

Hybrid warfare has to be carefully analysed and preparations have to be made for waging it. The Central European countries should devote particular attention to Russia. A fight against an opponent that wages a hybrid war is the task for the entire society and must be conducted in all areas. Last but not least, the society must be prepared to make hybrid counterattacks in the area of information war and in cyberspace against the attacker. However, in our opinion, a much more dangerous form of Russian aggression against members of NATO would be a repeat of the Georgian scenario, especially if it is supported by nuclear threats from Russia.

5. Proposed measures for improving the ability of states to face hybrid warfare

• Strengthen the state's ability to fulfil its basic functions and hence the loyalty of citizens to the state.

• Carry out intelligence and analytical activities in order to detect enemy preparations for a hybrid warfare, and, particularly, the launch of hybrid attacks using subversion.

• Continually single out countries that might resort to hybrid warfare and focus attention on them already in peacetime. Continuously draw up plans of countermeasures of both defensive and offensive nature against these countries in all areas relevant to hybrid warfare.

• Systematically prevent the infiltration of political leadership of the state carried out by agents of influence of a potential hybrid attacker.

• Acquaint the public in a suitable form with influence networks which a potential hybrid attacker constructs in the attacked-to-be country as well as with their modus operandi.

• Strengthen social cohesion of the country. By the active state policy do not allow the creation of variously defined socially excluded areas (e.g. based on ethnicity, religion or social status), which a potential attacker could rely on and which he could exploit in his campaign.

• Develop and build political relations with other potential targets of hybrid aggression. Exchange experience both on appropriate multilateral platforms (NATO and EU) as well as bilaterally.

• In the area of foreign policy, strive to address the threats associated with hybrid warfare in international organisations for collective defence of which the state is a member.

• Reduce to a minimum the necessary level of diplomatic, economic, military and cultural relations with countries that have been evaluated as potential hybrid attackers.

• Develop an adequate form of homeland defence consciousness and educational activities among the population concerning hybrid warfare and ways to face it. Systematically develop cooperation in this area with an authentic civil society.

• Enhance flexibility and the ability of independent action at all

levels of state, local government and the armed forces.

• Develop a wide range of capabilities needed for hybrid warfare, particularly intelligence capabilities, including the abilities to operate in cyberspace and to use information operations.

• Build military capabilities to be usable at all types of expeditionary operations and in defending territory.

• Strengthen the ability of the police to act against irregular and hostile unidentified armed formations fighting incognito at the very moment they attempt to paralyse the authority of state and local government.

• Create legislative conditions to ensure that police forces could be rapidly reinforced on the national territory by the military in their fight against unidentified armed formations at a time when the state has not formally been declared a war.

• Pursue scientific study of the issue of hybrid warfare using the approaches of all relevant scientific disciplines.

Research and presentation paper by Jagello 2000 in cooperation with Faculty of Social Studies, Masaryk University, Brno and European Commission Representation in the Czech Republic. This is an edited and translated version of a text published in Czech as "Hybridní válka jako nový fenomén v bezpečnostním prostředí Evropy" (ISBN 978-80-904850-2-0) in September 2015 by Jagello 2000. The original text was written by Zdeněk Kříž, Zinaida Shevchuk, Peter Števkov (Masaryk University, Czech Republic).

Jagello 2000

Jagello 2000 is a leading Czech non-profit civic organization active in public and defence diplomacy. Its main goal is to build a well-informed public that is more understanding in terms of defence, security, transatlantic relations and NATO. The main impulse to establish Jagello 2000 came with the 1999 membership of the Czech Republic and Poland in NATO. Jagello 2000´s flagship project is NATO Days in Ostrava & Czech Air Force Days – the biggest security show in Europe. Other key projects include the natoaktual.cz news portal, the Aliante international student competition and the NATO Information Centre in Prague. Jagello 2000 has been the representative of the Czech Republic in the Atlantic Treaty Association since 2003.

István Simicskó
Minister of Defence of the Republic of Hungary

The Visegrad Cooperation as a contributor to security and defence in Europe

Road to WARSAW SECURITY FORUM 2015

In February, 2016 the Visegrad cooperation will celebrate its 25th anniversary. Twenty five years ago, the four Central European countries signed a declaration in Visegrad to cooperate along their economic, diplomatic and political interests. Though, the Czech Republic, Hungary, Poland and Slovakia share common cultural, religious and historical roots, the purpose of this cooperation is not only to strengthen and preserve their heritage but also to contribute to build a European security structure within the Euro-Atlantic area.

Since 1991, many things have changed and today we have been witnessing a considerable change on the global security landscape. Among others, we have to cope with the crisis in Ukraine, the civil war in Syria, the unstable or even anarchic Sahel region and Central Africa and the mass migration from these regions to the European Union. We also have to take into account newly emerging threats, most importantly cyber threats, which are different from those of conventional threats and might necessitate a comprehensive review and amendment of our concepts of war. The cumulative effects of these changes might decrease the cohesion of the transatlantic community in a period when the global security environment is full of complex and dangerous challenges.

These global security circumstances made central European countries realize that a strong regional alliance is inevitable in order to tackle with the upcoming issues successfully. The European Union and NATO also encouraged close co-operation within the region which needs increased transparency. Both organization took steps towards a better cooperation on capabilities development, therefore they introduced the EU Pooling and Sharing and NATO Smart Defence concepts. The Visegrad Group realized its essential role in strengthening the ties between Central Europe and the Euro-Atlantic structure and full-heartedly supported the initiatives. In 2012 the V4 Defence Ministers presented a declaration of Responsibility for a Strong NATO in which they assured their commitment to further implementation of the 2010 NATO Strategic Concept. The declaration was followed by several other joint statements.

Moreover, the members of the V4 recognized that the region's interests are best articulated and represented in both the EU and NATO if our countries join together and

adjust their policies according to our common needs. Regular exchange of views on different security or defence policy issues became a standard practice. We have been thinking together, we have been issuing joint non-papers and declarations, addressing the most relevant topics on NATO's and EU's agenda.

When Hungary took over the rotational annual presidency of the Visegrad Cooperation from Poland in July 2013, a strong commitment to direct defence-related initiatives within the V4 towards a more visible and effective form of cooperation was clearly stated. Based on the achievements of the Polish Presidency, Hungary committed herself to facilitate the establishment of frameworks and political guidelines that enable the V4 to act on the European political scene with more visibility, credibility and with practical results. Thus, besides the bottom-up approach that characterised our cooperation in the past, a top-down approach to channel strategic intentions has been introduced, which manifested in the joint statement of our Prime Ministers in October 2013, Budapest Joint Statement of the Visegrad Group Heads of Government on Strengthening the V4 Security and Defence Cooperation. The highest political attention made the field of defence cooperation a flagship area within the V4 cooperation.

In 2014 March, the Long Term Vision of the Visegrad Countries on Deepening their Defence Cooperation stated our main objectives such as deepening of defence cooperation, modernization of our armed forces, better use of the available resources, and increasing/maintaining the level of defence spending. We considered the following areas especially important: capability development, procurement and defence industry, establishment of multinational units and running cross border activities, education and training and exercise. During the Slovak Presidency an Action Plan was finalized to help the implementation of the Long Term Vision which provided a good basis for the Czech Presidency and the next year Polish Presidency to take action.

The V4 EU Battlegroup soon became the flagship of the V4 defence cooperation. The importance of this project lies in its ability to show our commitment to contribute to the rapid response capability of the European Union and to give visibility to our cooperation, but most importantly to foster our common capability development. In November 2015, the V4 EU BG certification exercise is taken place linked to the NATO high visibility exercise "Trident Juncture 2015". The joint exercise provides the "V4 brand" with a better visibility and contributes to enhance NATO-EU cooperation.

Another successful achievement of ours is the development of Cross Border Operations between the four countries. Right now we are at the level of creating bilateral agreements, thus later we will be able to raise them to a multinational level. The agreement between Hungary and Slovakia can be signed this year and the agreements between the other V4 countries are at final stages as well. We are determined to develop our cross border regional cooperation according to the NATO Integrated Air and Missile Defence System (NATINAMDS) and the Single European Sky (SES) rules. In addition, we have recently started discussions about the possibilities of a future regional pilot training.

Defence planning is a relatively new field of our cooperation. The Visegrad Heads of State and Government gave guidance in their Joint Budapest Statement in 2013 to explore the possibility to create a framework for an enhanced defence planning cooperation. Since then, a structured and pragmatic collaboration has started with the aim of identifying promising areas for common capability development. This includes not just pooling and sharing of existing assets, and joint procurement projects, but cooperation among our defence industries, and research and development activities.

As for our future goals, we think it is crucial to utilize the experience we will have gained during the V4 EU BG 16 standby period. Our long term plan include the establishment of a permanent modular force and a V4 EU BG in 2019. The permanent V4 modular force is to be a real and genuine spearhead project of the Visegrád defence cooperation. Once it will be formed, it can provide us with an effective force-multiplier to contribute to NATO, EU and other international activities, while strengthening the V4 brand, as well.

Due to the increasing security challenges, the V4 countries expressed their intention to cooperate more closely in defence and security matters at political level as well. Currently, in the field of political consultations, our common goals include the representation of V4 priorities in the EU Global Strategy on Foreign and Security Policy, V4 preparation for the Warsaw Summit and dealing with the immense flow of migration. Though, in some cases our level of threats differs and therefore we might use different approaches, we try to address the challenges together.

In the run up to the Warsaw Summit, we have already started our work of preparation. The implementation of the Readiness Action Plan is the most important undertaking on the road to the Warsaw Summit. The common goal is to

complete all work strands by Warsaw. For us, a big step towards this goal was the recent ministerial agreement to set up two additional NFIUs in Hungary and Slovakia. Through this step, NATO's Eastern borders will be covered with small multinational headquarters, signalling the indivisible security of our Alliance.

Since the Eastern part of Europe is currently facing with numerous challenges, strengthening cooperation in areas where we have common interest is crucial. Mass migration towards the European Union is a key issue not only from a European but a regional perspective as well. The V4 is determined to manage the current migratory pressure in the framework of a regional cooperation and we all agree that the Schengen borders of the EU need to be protected. By contributing to the Hungarian border protection, the V4 countries expressed their political support for Hungary, but it is also a practical assistance for us which proves the effectiveness of the Visegrad Group.

I believe that regional cooperation within the EU and also NATO is an effective and trustworthy force that contributes not only to the strengthening of regional security but it fosters stability and security in Europe as well. Therefore, the V4 is determined to move ahead on this road and it is also open to cooperate with other regional formations such as the Central European Defence Cooperation (CEDC). Some forms of consultation and co-operation already exists with the Weimar Triangle and NORDEFCO as well, but we are ready to seek new opportunities for V4 + W3 co-operation within the EU and NATO. We are also open to further explore how we could work together with the US.

The Visegrad Group is a strong strategic partnership in a region with strategic importance, democratic values and a strong will to cooperate in the hope of a more secure world. V4 co-operation, serving as a model for regional co-operation, has proved to be a 25-year-old friendship with great determination to support regional development and European stability.

István Simicskó

Minister of Defence of the Republic of Hungary

Following the landslide victory of the Fidesz in the 2010 parliamentary election, Simicskó was appointed Secretary of State for Defence on 2 June 2010, under Minister Csaba Hende. Simicskó was appointed to the position of Minister of Defence in September 2015 after the resignation of Csaba Hende during the European migrant crisis, with the speed at constructing a wall on the border with Serbia being an issue for Prime Minister Viktor Orbán.

Joanna Świątkowska
CYBERSEC Programme Director
Senior Research Fellow of the Kosciuszko Institute

Cybersecurity - fundament of overall safety and security within the European Union – state of play and future, and future challenges

Road to WARSAW SECURITY FORUM 2015

It has been more than two years since the adoption of the Cybersecurity Strategy by the European Union. It is a good time to look closer at actions taken by the European Community and identify at least some challenges that will need to be faced in the nearest future.

The document sets out the principles for cybersecurity as well as points out the EU vision, articulated in five strategic priorities:

1. Achieving cyber resilience,

2. Reducing cybercrime,

3. Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy,

4. Developing the industrial and technological resources for cybersecurity,

5. Establishing a coherent international cyberspace policy and promoting core EU values.

Starting with the first strategic priority, there are numerous actions and initiatives currently undergoing within the EU that help to achieve cyber resilience. In this context, the role of the European Network and Information Security Agency cannot be underestimated. The Agency supports the stakeholders in various activities which aim to increase the cyber capabilities. Among many others, ENISA presents recommendation and good practices in preparation of robust cybersecurity strategies and implementing actions that help to increase cybersecurity. Even though more and more EU countries are increasingly taking actions that should assure higher level of security in cyberspace, there are still gaps across the EU. National capabilities (quality of cyber initiatives, solutions) are not strong enough, and very often leave much to be desired. Many of the EU countries must also improve their relations in terms of cooperation. Building widely understood solid cyber capabilities at the national level is the goal that needs to be achieved as soon as possible.

Even though this process requires involvement of many different stakeholders, one element of the system should be underlined. CERTs (Computer Emergency Response Teams) play increasingly important role in the ecosystem of cybersecurity. Even though Member States as well as the EU itself develop these entities, building stronger capabilities and cooperation between them is crucial. CERTs' community should work together even stronger and share good practices, exchange experiences multilaterally and bilaterally – not only within the EU but also beyond. For instance, cooperation with Ukrainian entities is currently very important.

One of the most important elements of the current EU activities is a Directive on a common high level of Network and Information Security (NIS) across the Union, related to national capabilities and preparedness, EU-level cooperation, take-up of risk management practices and information sharing. The legislation will establish minimum requirements for network and information security at national level, and will oblige Member States to take numerous actions in the field of cybersecurity. Currently, the NIS Directive is negotiated at the EU level. Many stakeholders count on this legislation, hoping that it will accelerate needed actions within Member States. Indeed, the document may have very positive influence on overall cybersecurity. Therefore, it is crucial to finish the process of the negotiations and adopt solid Directive. At the same time, however, Member States cannot wait passively for international solutions. There is a strong need to take actions right here, right now.

The foundation of the cybersecurity is based on well working, efficient private-public cooperation. The EU is making strong effort to enhance this type of cooperation. European Public-Private Partnership for Resilience is one example of this engagement. But again, more decisive actions at national level are required. The main dispute concerns whether to build this cooperation on mandatory or voluntary approach and how to build trust between different actors. Regardless of the chosen approach, well organised and planned system of effective incentives (financial and non-financial) that would boost the cooperation is needed. Some propositions and recommendations in this area can be found in the report Critical Infrastructure Security – the ICT dimension – prepared by the Kosciuszko Institute.

The second aim of the Cybersecurity Strategy of the European Union is to drastically reduce cybercrime. There are at least two international instruments that strongly help to achieve this goal. The first one is establishment of the European Cybercrime Centre and the second is existence of the Council of Europe's Budapest Convention on Cybercrime. Combating cybercrime effectively requires developing relevant skills at the domestic level with international cooperation. All the stakeholders, especially entities responsible for law enforcement and the judiciary must adjust their modus operandi to the new, digital environment. The actors must have new powers and tools to perform their duties sufficiently. Next step is to use joint efforts to fight cybercrime globally – to increase efficiency of actions and eliminate safe havens. Above-mentioned: the EC3 and the convention are fundamental. The Centre must further develop its capabilities, and

the international community must find ways to implement the Convention's provisions more fully and to promote its ratification by other countries. The other challenge is to keep the document up to date, to keep up with the changing reality.

Next strategic priority is related to the development of cyberdefence policy and its capabilities. In context of this strategic issue, it is significant to underline cooperation with NATO. It is extremely important to harmonise efforts of these two organisations and avoid any duplications. Only by understanding different roles and responsibilities can we achieve the effect of symbiosis. This cooperation, for instance, can be materialised in more intense collaboration in the field of critical information infrastructure protection, more intense exchange of information, early warnings and other good practices.

Having said that, the EU decision-makers must understand thata more and more tense geopolitical situation in Europe – conflict in Ukraine, hybrid warfare that includes cyber elements, cyber operations of so-called IS – poses increasing challenge and takes relevant actions. Nowadays, almost all conflicts that take place in real word have some elements that are performed in cyberspace. These elements have different dimensions and various consequences. The nature of this challenge must be understood and taken under consideration while thinking about the European security and safety.

Cybersecurity not only ensures our well-being and functioning of our daily lives but it is also the backbone of the EU economy. In this context, it is worth mentioning that the European Commission has identified the completion of the Digital Single Market (DSM) as one of its ten political priorities. By achieving this aim Europe can boost its GDP by almost €500 billion a year. The preconditions of successful actions within the DSM framework are cybersecurity and consumer confidence. This argument is supported by data: 38% of the EU internet users are concerned about the safety of online payments and have consequently changed their behaviour regarding security issues, 18% declare to be less likely to buy goods online, and 15% affirm that they are less likely to use online banking .For these reasons additional actions are needed – citizens must have trust in ICT products and services.

Cybersecurity cannot be assured without technological and human resources. Strong research, development, and innovation in the field of cybersecurity are the fourth priority. Europe needs ICT products and services that are trustworthy, secure, and guarantee the protection of personal data. Therefore, it is highly important to stimu-

late further financial investments and development of the market that will demand for highly secure products. One recommendation herein will be to design framework of security standards that would help to increase cybersecurity. Industry-led, sectorial cooperation in this area is fundamental. Regarding the financing - it requires mobilisation of national resources as well as skilful use of European funds. There is a need for political decisions which will acknowledge the importance of cybersecurity and delegate budgets on this aim. Stakeholders must also learn how to forcibly take advantage of the opportunities offered by, among the others, Horizon 2020.

However, cybersecurity cannot be achieved only by taking actions at the European level. Due to the global nature of the internet and cooperation, it is fundamental to start building cyber capabilities beyond the EU. Cyberspace entered the arena of international relations. It became an important element of debates between most powerful actors. Decisions that will be made regarding numerous cyber issues will influence the daily functioning of all the actors. Recognising the importance of the problem, the EU decided to mainstream cyberspace issues into the EU external relations and Common Foreign and Security Policy. The European voice must be heard. This can only happen if the Member States itself will develop capabilities in the field of cyber diplomacy. Combination of domestic and European efforts is the key for the success.

In order to provide cybersecurity globally, Europe must cooperate with like-minded countries. At the same time, decision-makers cannot forget about looking for consensus with actors which might not share the same vision of cyberspace.
Currently, the crucial and needed transatlantic cooperation in the area of cyberspace is facing many challenges. Revelations of Mr. Snowden have disrupted trust and confidence between the Allies. These virtues must be restored while thinking about future cooperation. Both sides need to understand each other's' positions and arguments, and respect their rights and privileges. Privacy and data protection is a central element. But even though these problems exist and must be resolved, we need to understand that both sides need each other and we cannot afford to act separately. The net gave power and possibilities both for good and bad actors. New challenges require new forms of actions where cooperation is absolutely essential.

According to what has been pointed out, the European community takes numerous actions to increase overall level of security. Many of the necessary steps are still ahead of us. Complexity and interdependences of cyberspace

require multidimensional decisions and initiatives both at the domestic and international levels. In order to prepare and implement solid actions, we need to understand that this old-fashioned approach is not valid anymore. We need to combine interests and efforts of different stakeholders. The Cybersecurity Strategy of the European Union with its multilevel approach is a proof confirming this conviction. Now, besides having the document in force, it is high time to take solid actions.

Joanna Świątkowska

CYBERSEC Programme Director
Senior Research Fellow of the
Kosciuszko Institute

Ms Świątkowska is cybersecurity expert at the Kosciuszko Institute's and director of CYBERSEC. She has been involved in numerous high profiled national and international cybersecurity initiatives. She often cooperates with Polish public institutions, including among others the Polish Presidential National Bureau of Security (NBS). In the framework of the National Forum of Security organized by NBS, she contributed to the cyber doctrine of Poland.

Andrzej Kozłowski
Research Fellow
Casimir pulaski Foundation

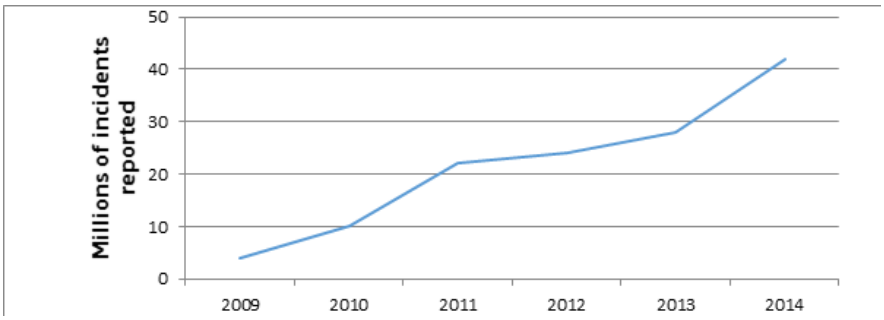
The cyber strikes back – the retaliation against the cyberattack

Road to WARSAW SECURITY FORUM 2015

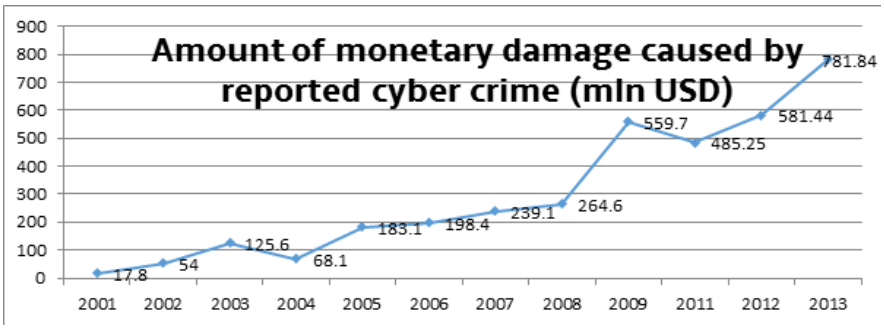
The growing threat

The constant grow of threats in cyberspace both in number and in sophistication has challenged the governments of many countries in the world. The billions of dollars lost every year because of the cybercriminal activity, the amount of data stolen by digital spies and more and more aggressive using of the Internet as a tool of propaganda have become the today reality.

Despite the fact that last years did not bring new breakthrough incidents comparable to the Stuxnet – first computer program able to inflict damages in material world, the impact and scope of cyberattack significantly rise up. Compromising of the Office of Personnel Management (OPM) data security,



Source: Assesing Cyber Security. A meta-analysis of threts, trends, and responses to cyber attacks received from http://www.hcss.nl/reports/assessing-cyber-security/164/



Source: David Liu, Cyber Criminals More Powerful Than Ever, New Report Claims, http://www.moneyeconomics.com/headlines/cyber-criminals-more-powerful-than-ever-new-report-claims/

announced by American media as the most serious breach in history of the United States or the hacking of Barack Obama's email box illustrates the threat coming from the virtual world. Furthermore, the cyber blackmail against Sony, which compelled this company to withdraw the comedy about North Korean leader shows the increasing danger for both private and public sectors.

For the long time governments have ignored the threats in virtual reality and limited their actions to arresting criminals for different cybercrimes. However, many cases that recently appeared were linked with hostile activity of the states and that factspurred debate among the policymakers how to react effectively on this issue. Nevertheless, it is extremely difficult to do it because of the several issues, of which the attribution remains the most challenging.

The problem of attribution

One of the main problems to retaliate effectively against the authors of cyberattacks is attribution. The architects of global network did not think about security issue when they projected the Internet. Initially it was created as the tool to establish communication between the military commands in the United States and later also to embrace the American academic entities. None in that time was planning global expansion. This construction's flaws lead to the situation that the cyberspace has become the oasis for the illegal activity. Initial cases of hostile activity were dominated by the young teenagers desire to earn extra money.

However, at the beginning of the 21st century more and more advanced, long-time incidents took place and countries, particularly the United States started to treat cyberattacks as the serious threat for national security. Several countries, especially Russia and China were accused of standing behind the attacks, which both of them strongly denied. Unfortunately, the problem of the identification of the assailant has seemed unresolved till today due to the architecture of the cyberspace. We are able to trace the IP addresses, which identify the computer in virtual world, but manipulating them remains simple and available even for beginners. That it is a reason that attack conducted against the United States from Chinese addresses did not mean that were orchestrated by Chinese but they might be a work of Russians or Israelis hackers using the IP located in China.

Despite aforementioned difficultness, the American private company Mandiant collected data and published reports accusing the Chinese military unit 61390 located in Shanghai of conducting

a bunch of cyber espionage campaigns against the US. The proofs were solid but the report remains a positive exemption among attempts to identify attackers. It is worth mentioning also how hackers were identified. American IT security experts under the leadership of Mandiant Company used the exploit in Chinese hackers' security networks and got access to their systems collecting logs and tracking every move then creating the digital diary. What is even more interesting, it was purely private initiative without the government engagement. Although the Mandiant report is the only known source clearly pointing out the assailants, there are several theoretical models of attribution of attack based on the social and political background. One of them, Jason Healey methodology consists of 14 factors. Using this methodology the last two OPM and Sony attacks will be analyzed.

The aforementioned examples show that both technical and political attribution is abundant with flaws and problems and only in special, very rare cases it is possible to be certain about aggressor. In other words, putting country such as Russia behind OPM hacking will bring similar results. In most cases there are speculations and lack of hard proofs and because of it the retaliation may extremely dangerous, when we aimed at impropriate country.

The possible scenarios of retaliation in cyberspace and in real world

Despite the uncertainty linked with the identification process of assailants state authorities prepared a range of tools used to retaliate. Part of them we could observed in certain cases, which happened in the past. When other appeared only in doctrines and strategies and never materialized in real world. Generally we can separate the retaliation in real world and in cyberspace. According to the international law states should use proportionate measures but it does not always happen.

In cyberspace

The most reasonable option should be answering in virtual world by using the similar tools and methods as the opponent. In the past, there were several cases illustrating the proportional retaliation. In 1999 during Kosovo war Serbian hackers attacked the NATO websites using the Denial Distributed of Service Attacks (DDoS). In response Western hackers affiliated and sympathized with mission also orchestrated the flooding type attack on the Serbian administration website. Similar cyber skirmishes happened during 2001 Chinese-American crisis over the crash between

Analytical Element	*OPM*	*Sony*
Attack Traced to Nation	Many traces to China	Many traces to North Korea
Attack Traced to State Organizations	Some Traced	Some Traced
Attack Tools or Coordination in National Language	No information	No information
State Control over the Internet	High	Very High
Technically Sophisticated Attack	Medium	Medium
Sophisticated Targeting	No	No
Popular Anger	Low	High
Direct Commercial Benefit	Very High	None
Direct Support of Hackers	Low	High
Correlation with Public Statements	Moderate	Very High
Lack of State Cooperation	China refused to cooperate	North Korea refused to cooperate
Who Benefits?	Chinese government and companies	Noone
Correlation with National Policy	High	High
Correlation with Physical Force	Moderate	Moderate

Source: Jason Healey, A fierce Domain: Conflict in Cyberspace 1986 to 2012, p. 265 – 276.

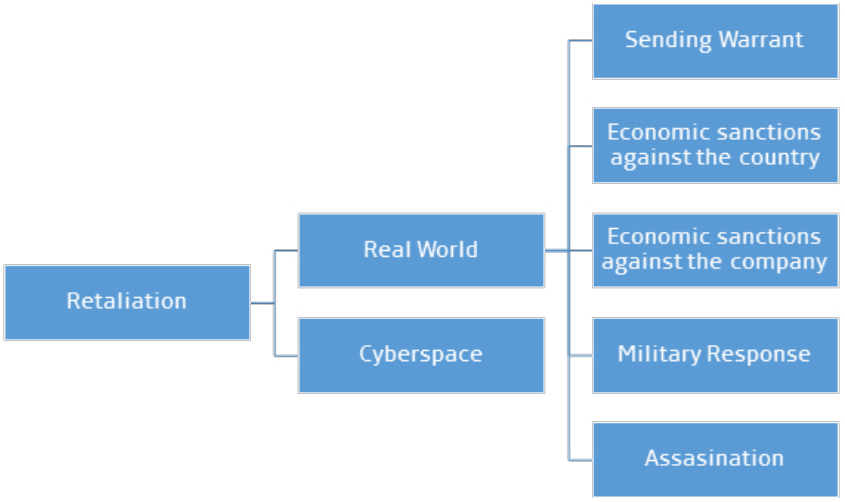
the Chinese jet and American spy plane or between the hackers of conflicting sides like Pakistan and India or Israel and Palestinian.

There is slight difference in the Iranian attack on the United States banks in 2012. It was retaliation for the Stuxnet worm, which infiltrated the Natanz uranium enrichment facility and destroyed thousands of centrifuges. This computer program became the first inflicting damages in the material world. However, Iran's abilities were too limited to conduct similar operation against the US and they decided to attack vulnerable sector – American banks. This response was not proportional. The response was far less destructive and limited only to digital world.

The retaliation in cyberspace is the most popular and probably will remain in the foreseeable future. The easy ways to carry out this kind of operation, the relative small consequences in case of the mistake and last but not least the problems with attribution encourage actors to these actions. The only weakness lies in the relative small damages brought by the retaliation in cyberspace.

Real World

For the long time the response for cyberattack in real world has remained only the deterrent tool recorded in different doctrines and strategies. But the last American operations showed that the response for hostile operations in cyberspace does not touch only this area. There are several options of retaliation in real world against cyberattack.



The cyber strikes back – the retaliation against the cyberattack

Military response

The strongest and harshest way of response is to conduct the military strike against country who conducts the hostile operations in cyberspace. This kind of operation never happened in history but e.g. United States and NATO officially declared that among retaliatory options they declared the possibility of military attack. On the last NATO summit in 2015 Wales there was statement in the end declaration that cyberattack could trigger the article V and therefore possible military reaction. The United States officially announced this option in the International Strategy for Cyberspace from 2011. There is no precise record about the conditions and situation of executing military attack but it is commonly recognized as the response to cyberattack with the magnitude comparable to conventional attack with the death tolls. It is very small chance of observing such a situation in the future. Mainly due to the fact that devastating cyberattacks are part of Hollywood movies, which are far from reality. What is more, the country that decided to conduct such a strike will change the history because the consequences can be unimaginable and extremely politically costly.

Assassination

The option of killing the talented hacker who is conducting the cyberattack seems more from the books and movies actions than from reality. Despite the fact, that it seems tempting to eliminate the most skillful and knowledgeable hacker, tno information of such attempt exists. The Tallinn Manual, which is recognized as the most ambitious attempt of adopting international law to cyberspace does not give a clear answer on this issue. It claims that during the peacetime it is forbidden, but it is not clear whether assassination of the hacker supporting and working with terrorists is forbidden too.

Untill 2015 this discussion was held on the solely theoretical ground but since August we had one practical case. The ISIS hacker Abu Hussain al-Britani, originally from Great Britain, created a network of hackers working for Islamic States. He personally was responsible for stealing and publishing the thousands of the U.S. military and government personnel documents, creating malwares and other hostile action. Al-Britani was killed by American drone in pinpoint attack. According to the Wall Street Journal this attack was deliberately aimed at killing al-Britani.

First time the hacker was killed because of his actions against the state. Al-Britani performed typical cyberespionage actions, which are done by most of the hackers both representing states and non-state

actors. There is no guarantees that further incidents will not happen, which constitute a grave threat especially in the hands of the authoritarian states. We can imagine similar assassination of the hackers, who fight for freedom in Russia, China or Iran.. Such a situation could occur repeatedly, because aiming talented individuals from the countries or organizations which cyber potential is limited is relatively easy and effective.

Arresting or Sending Warrant

Arresting the cybercriminal was the first method used against persons engaged in hostile activity in cyberspace. In 90s it was relatively easy because most of the attack was orchestrated from territory of the United States. In the 21st century this situation has changed and pursuing cybercriminals becomes more and more complicated. However, the international and bilateral cooperation contributed to catching famous Max "Iceman" Butler and the Dark Market heads and this cooperation is still used and developed e.g. under the Convention on Cybercrime.

But in 2014 the United States went even further and filled criminal charges against five Chinese military officers for stealing trade secret. This kind of situation happened first time in history and obviously could not achieve success but it presented determination of the US authorities and also the fact that they are more and more upset with increasing Chinese engagement in cyberspace activities. The accusations were rejected by government in Beijing and obviously the chances that these 5 people will be sent to US are very low, but it was a signal to Chinese government to reduce their involvement in cyberespionage campaign and that United States government treats it seriously.

The attempt to arrest hackers who break the law will be the most common and widespread method used in future. However, it requires the development of forensic tools to present proofs sufficient to prosecute and imprison persons responsible for cyberattack

Economic sanctions against the company

The situation when the economic sanctions were imposed against the particular companies has not happened yet, however this option was considered. Just before the last summit between president Obama and Chinese president Xi Jinping the media speculated that United States would impose sanctions against the Chinese companies, which gained the largest benefits from the cyberespionage campaigns. This solution seems as the interesting option but measuring profits received by certain

company still remains difficult issue to solve. Moreover it is difficult to image that the small countries can use this tool against gigantic IT companies like Apple or Microsoft. Nevertheless, in the foreseeable future this tool can be used because it has not constituted the grave treat and can be treated as the effective deterrence mean.

Economic sanctions against the state

Not only can the certain companies be punished by the economic sanctions but also the states. This happened in case of North Korea, which was accused of massive cyberattack on Sony and in consequences forced the company to withdraw comedy movie about the North Korean leader from the United States cinemas. Barack Obama's administration decided to impose additional economic sanctions on North Korea and therefore setting precedence. This decision was mostly symbolic as the North Korea was imposed with multiple sanctions in the past and remained one of the most isolated countries in the world. But the American decision was more than just to punish Kim Dzong Un regime and should be understood as deterrence action illustrating the feasible US response.

However, there are three danger points pop up regarding with this solution. Firstly, the United States did not show any proofs pointing out that North Korea was behind the attack, which seems dangerous as some countries can use these tools for political purpose. Secondly, it is hardly imagine that small country imposes sanctions on the more powerful countries e.g. Estonia or Georgia using this tool in 2007 or 2008 against Russia. Third point relates with the previous one, that economic sanctions are the double-edge sword and in certain situation can be more harmful to the country, which decides to impose them.

Conclusion and recommendations

The surprising assertiveness of the United States. The recent time was abundant with the examples of retaliation for cyberattacks especially in the real world. Particularly the United States set precedence over precedence and reacted very aggressively. This kind of behavior rather does not fit to Obama administration recognized rather as consisted of doves than hawks.

- Increasing the number of tools to retaliate in cyberspace. US policy in cyberspace created several options to retaliate and what is even important to deter the cyberattacks. It is too early to conclude whether they were effective or not but obviously constitute important points in

discussion about cyberattacks. Nevertheless, the American operations were also reckless and might open the Pandora box, like Stuxnet did in the past.

• Lack of proof. The United States did not present publicly any proof indicating that certain state, in this case, the North Korea was behind the attack. It may lead that countries will use this option to achieve particular political option. The scenario that one country accused the second one of conducting cyberattack and it is imposing economic sanctions seems as plausible and considering the problem with attribution can be really dangerous.

• Legal Controversies. The assassination of the hacker also from the legal point of view is very controversial and unclear. The United States preforming such an action should prepare the legal opinion on this issue and publish it just after the attack. In this way they can contribute to development of the international law in cyberspace.

• Lessons for Poland. Poland must be aware of the new tools used in cyber retaliation and be ready for them. There should prepare scenarios of different reaction and also the mechanism of deterrence. In order to realize these aims Poland needs to develop own cyber offensive capabilities and creates the effective mechanism of executing them. The public confirmation of possessing such capabilities should be considered as the good deterrence option.

Andrzej Kozłowski

Research fellow
Casimir Pulaski Foundation

PhD candidate at the International Studies and Political Science faculty of the University of Łódź. Graduated from International Relations Faculty of the University of Łódź. Scholarship holder of the Erasmus programme at the University of Maastricht in the Netherlands. Expert of the Amicus Europae Foundation and the Kosciuszki Institute. Former intern at the Polish Institute for International Affairs (PISM), National Security Bureau, European Parliament, Polish Embassy to Netherlands in the Hague and the European Institute in Łódź.

WARSAW SECURITY FORUM

2015

Project of

CASIMIR PULASKI FOUNDATION

warsawsecurityforum.org | facebook.com/WarsawForum | twitter.com/WarsawForum