Civil-Military Cooperation
Centre of Excellence
The Hague

Resilience

A CCOE Fact Sheet

What is Resilience?

Why Resilience?

What type of Resilience? Resilience for whom?

- Individual;
- Societal;
- State;
- Regional and Global Resilience.

From which threats?

- Natural disasters/hazards
- Man-made disasters/hazards
  - ➢ Terrorism;
  - ➢ Cyber;
  - ➢ Hybrid threats.

What are the key organizations?

- NATO;
- EU;
- UN.

What is NATO's approach to Resilience?

- Seven baseline requirements
- NATO's contribution to Resilience (CEPCI)
  - ➢ Cyber Defense;
  - ➢ Hybrid threats;
  - ➢ Cooperation with EU;
  - ➢ Cooperation with partner countries;
  - ➢ Civil-military readiness.

WWW.CIMIC-COE.ORG

What is Resilience?

Resilience is a comprehensive and relatively new concept that has received attention within many disciplines and fields.

Resilience was first introduced within the field of ecology in the 1970's.[1] Afterwards, its use expanded to other disciplines, such as psychology, environment, organizational management and economics.

In the past decades, the resilience concept has entered a wide range of security discourses, and has been applied in fields such as disaster preparedness, counterterrorism, critical infrastructure, cybersecurity and many others.[2] Applied to many disciplines in a short time, the concept of resilience has become a solution to many challenges in security and governance.[3] It has been described as "a system's emergent response to emergencies"[4]. Resilience can be described as the capacity to withstand and recover from shocks, absorb damage, resume function as normal as quickly and efficiently as possible following extreme disturbances.

A resilient system maintains stability and safety[5]; diminishes the possibility of failure; reduces consequences of disturbances and speeds up the recovery period.[6] It comprises both "Pre" -preparedness and "Post"- response to disturbances.

Why Resilience?

Today, we live in a complex security environment. The frequency and severity of threats continues to increase, and new threats and hazards are constantly emerging.

In the environment where the threats are complex and unpredictable, it is impossible to guarantee complete security. Current threats do not only impact human lives, but also economic and social development as well as security environment of states.

This dynamic environment requires comprehensive precautionary measures. Simply reacting to a disaster or crisis is no longer seems sufficient; a more preventive approach is needed. Due to that, it is more effective to identify and address the root causes of threats than dealing with their consequences. The rehabilitation period of states and communities after the disasters and crises increasingly require more time and resources. In the long term, building resilience would be more effective, and with time, also cost-efficient.

Resilience can strengthen the capacity of individuals, communities, but also states towards disruptive events. [7] Even though complete protection from those events may sometimes not be feasible, resilience can help preparing to withstand those disturbances, and quickly recover from their effects.

[1] Walker, J. and M. Cooper. 2011. Genealogies of resilience: From systems ecology to the political economy of crisis adaptation. *Security Dialogue*. *42*(2): 143-160

[2] Cavelty MD, Kaufmann M, Kristensen KS (2015) Resilience and (in) security: practices, subjects, temporalities. Security Dialogue 46(1): 3–14

[3] Aradau, C. (2014). The promise of security: resilience, surprise and epistemic politics. Resilience, *2*(2): 73-87.

[4] M. Kaufmann (2016) Emergent self-organization in emergencies: resilience. Security Dialogue *47*(2): 99 –116

[5] Cavelty MD, Kaufmann M, Kristensen KS (2015) Resilience and (in) security: practices, subjects, temporalities. Security Dialogue *46*(1): 3–14

[6] Tierney, K. and Bruneau, M., (2007) Conceptualizing and Measuring Resilience: A Key to Disaster Loss Reduction. TR News 250: 14-17

[7] Cavelty MD, Kaufmann M, Kristensen KS (2015) Resilience and (in) security: practices, subjects, temporalities. Security Dialogue *46*(1): 3–14

Resilience for whom?

Considering the diversity of threats and their targets, resilience can be observed at different levels of society. All levels are interconnected and influence each other.

Individual resilience is demonstrated by the ability of individuals to withstand changes, adapt to and recover from traumatic events. Individuals may face shocks such as stress, social disorder, poverty, loss of family member or a job. Individuals with strong resilience are healthy, less susceptible to stress and have an ability, skills, and knowledge to cope with challenges and disturbances. Resilient individuals also participate in community resilient efforts, as well as contribute to the overall state resilience.[8]

Societal resilience is demonstrated by the capacity of community to prepare for hazards, diminish and prevent damages to people, property and environment, restore the basic services and function effectively in the aftermath of disturbances. A resilient community is self-mobilized, has an efficient and effective infrastructure and is able to respond to hazards by utilizing its own resources. Members of a resilient community are well connected, educated, and disaster-prepared.[9]

State resilience is demonstrated by a "state's ability to withstand or recover from strategic shocks that stress and possibly distort state institutions and political settlements".[10] State resilience tackles the issues related to the rule of law, governance, infrastructure and social security systems. The hazards that pose challenges can be "internal or external, natural or orchestrated or as part of a hybrid attack".[11] In this respect, building and enhancing resilience requires collaboration between civilian, economic, private and military factors. By taking long term resilience measures, a nation state can diminish expenses, time and human lives connected to a threat, and return to the previous state of function without any major problems.[12]

Regional and global resilience is demonstrated by the ability of cooperating regionally or internationally to address regional or global hazards such as conflicts, disasters, climate change, hunger, mass migration, diseases as well as cyber and hybrid threats. A number of regional and international organizations are strengthening the capacity of regions and states with a range of programs and projects to help build resilience against future hazards.[13]

From which threats?

In today's world, we face an unprecedented range of security challenges. In order to combat those challenges, a simultaneous response to all hazards - both natural and man-made – would be required.[14] Natural disasters include earthquakes, hurricanes, tsunamis, wind storms, avalanches as well as epidemics, while man-made disaster can be complex emergencies/conflicts, famine, displaced populations, industrial/transport accidents, terrorism, cyber, and hybrid threats. The most current and likely threats will be discussed below.

[8] IFRC(2014) IFRC Framework for Community Resilience

[9] Norris FH1, Stevens SP, Pfefferbaum B, Wyche KF, Pfefferbaum RL.(2008) Community Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness, Am J Community Psychol, ;41(1-2):127-50.

[10] CCOE (2017) A Civil-Military Response to Hybrid Threats to be published

[11] Ibid

[12] Ibid

[13] IFRC(2014) IFRC Framework for Community Resilience

[14] Dainty ARJ and Bosher LS (2008) Integrating resilience into construction practice. In: Bosher LS (ed.) Hazards and the Built Environment: Attaining Built-in Resilience. London: Taylor and Francis

Natural Disaster:

The impact of each disaster is immense, as disasters have a direct effect not only on individuals and communities (such as death toll and infrastructure damage), but also a continuous effect on the social and economic situation of the state and region. In the last decade, thousands of people lost their lives, millions have been injured, became homeless or displaced by disasters. Total economic lost is estimated to be $1.3 trillion.[15]

Even though the duration of a disaster usually does not exceed more than a couple of days, the consequences and destruction caused by that disaster may take considerably longer to remediate. Furthermore, due to several global factors, such as climate change, population growth, urban migration and shortage of natural resources, the frequency and magnitude of disasters are expected to increase in the upcoming years.[16]

Taking effective resilience measures to unforeseeable disasters has become one of the primary global concerns. Building and enhancing resilience can diminish the impact of disasters and the destruction that follows. Moreover, it prepares individuals, communities and states to cope with potential future disasters and to have the capacity to return to normal life after a disruptive event. Building disaster resilience involves measures, such as:

- strengthening disaster governance;
- creating awareness and disaster preparedness among the population;
- improving early warning systems;
- introducing disaster risk management policies and programs;
- enhancing international cooperation between actors;
- Identifying and reconstructing disaster prone infrastructure.[17]

Man-made Disasters:

Terrorism

9/11 terrorist attacks marked a turning point for not only history of United States, but the whole world. Despite the fact that terrorism wasn't a new phenomenon, after 9/11 it became a pressing topic which required the introduction of new laws and policies for countering terrorism. Terrorism was no longer the problem of a single state. Because of it, 'national security' and 'international cooperation' became interconnected terms in order to fight international terrorism.[18]

Individuals, nationalist or religious groups can be involved in terror related activities for a variety of reasons, and come from various ideological backgrounds. The background of the terrorists shows that it is not only coming from abroad, but can also be homegrown as a cause of radicalization.[19] Terrorists can have political and social motivations, such as gaining political influence, obtaining global recognition, or affecting a country's economy and security infrastructure. Throughout history, terrorist groups have targeted politicians, police, public officials, and foreign embassy staff by using different methods, for example, assassination, hijacking, kidnaping and suicide bombing.[20] Today the victims of the terror attacks are civilians rather than military or political figures.

[15] UNISDR (2015) Sendai Framework for Disaster Risk Reduction 2015 – 2030
[16] DFID (2011) Defining Disaster Resilience: What does it mean for DFID?
[17] UNISDR (2015) Sendai Framework for Disaster Risk Reduction 2015 – 2030
[18] Rogers P. (2008) Terrorism. *Security Studies: An introduction,* Taylor & Francis Group
[19] Veldhuis T. & Staun J. (2009) Islamist Radicalisation: A Root Cause Model. The Hague: *Netherlands Institute of International Relations Clingendael*
[20] Rapoport, D. (2004) 'The Four Waves of Modern Terrorism', in A. Cronin and J. Ludes (ed) Attacking Terrorism: Elements of a Grand Strategy, *Washington DC: Georgetown University Press*, 46-73

The consequences of terror attacks can vary from causalities to infrastructure damage and economic loss. Additionally, it disturbs and endangers the security system of the state as a whole. Terror attacks also create a sense of fear among the population that leads to a change in personal behavior like increased ethnocentrism and xenophobia.[21]

Building resilience against terrorism includes combating its root causes such as preventing radicalization, improving awareness of the population to security issues, promoting inclusivity and diversity of the society, enhancing the cooperation and dialogue between international actors.

Hybrid threats

Contemporary conflicts are no longer classified as traditional or irregular. Today, the lines between war and peace, regular and irregular forces, combatant and non-combatant, physical and virtual are increasingly blurring.[22]

Nowadays, enemy intentionally target the weak points of opposition by using both conventional and unconventional means such as terror, propaganda, separatist activities, and cyber-attacks in order to achieve their specific objectives. Hence, the emerging nature of contemporary conflicts became more complicated than only involving military power.

These threats that pose challenges to the contemporary security environment are called hybrid threats. “Hybrid threats incorporate a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder”.[23] Both state and non-state actors with or without state funding can be involved in conducting hybrid threats.

NATO identified hybrid threats as “multimodal, low intensity, lethal and non-lethal threats to international peace and security including cyber war, low intensity asymmetric conflict scenarios, global terrorism, piracy, transnational organized crime, demographic challenges, resources security, retrenchment from globalization and the proliferation of weapons of mass destruction.”[24]

Although hybrid threats violate the law of armed conflict and international law, due to their complex and contemporary nature, hybrid threats are not regulated by any international legal framework. This makes countering hybrid threats a challenge.

The rise of hybrid threats does not indicate the end of traditional conflicts, however, it does require the comprehensive approach for countering and withstanding attacks by using all available economic, political, diplomatic, technological, as well as intelligence tools.[25]

[21] Huddy, L, Feldman, S, Capelos, T and Provost, C (2002) The consequences of terrorism: Disentangling the effects of personal and national threat, *Political Psychology, 23* (3). pp. 485-509.
[22] Hoffman F .G. (2007), Conflict in the 21st Century: The Rise of Hybrid Wars, Arlington, VA: Potomac Institute for Policy Studies, 8
[23] Ibid
[24] CCOE (2017) A Civil-Military Response to Hybrid Threats.
[25] Ibid.

Cyber threats[26]

In addition to conventional threats, nowadays cyber threats are growing in frequency, sophistication and scope, becoming increasingly more damaging. The actors engaged in cyber activities can vary from individuals to hacktivist groups, but also include government organizations. Using sophisticated and powerful IT techniques, these actors penetrate the computer networks of individuals, organizations, businesses as well as state agencies. The scope of coordination and complexity required for a cyber-operation is usually indicative of the actor involved. The larger and powerful supporters (sponsors) are behind the more complex and bigger operations. Those high-powered operations are most likely funded by state entities.

Cyber-attacks may have different motivations and goals. It can be used for espionage, sabotage related activities, infrastructure damage, financial gain as well as for reaching political goals. In general, the target of espionage and sabotage related cyber operations is confidential and sensitive information. Acquiring sensitive and secret information allows achieving strategic objectives against adversaries, and provides a clear advantage. In addition, it also benefits political and military goals of the opposition (adversaries). Cyber threats can take advantage of existing vulnerabilities and affect critical infrastructure, energy and transportation system. This can result in massive revenue loss and damage to economy and stability of a state.

Enhancing resilience against cyber threats requires identifying risk and threat landscape, keeping pace with rapidly changing technologies, engaging with countries, organizations as well as private cyber security sector, exchanging cyber defense related information with partners, introducing training and exercises in order respond to and adapt security challenges.

Which organizations are involved?

NATO

Resilience is not a new concept for NATO. It was introduced during the Cold War to reinforce and maintain the capability of nations to be resistant during war and crisis situations. However, in order to tackle rapidly emerging threats and improve NATO's deterrence and defense capabilities, the NATO Readiness Action Plan was introduced at the 2014 Wales Summit. Taking into consideration the threats and vulnerabilities, minimum standards for national resilience have been agreed.[1] Therefore, seven baseline requirements considered the most critical to NATO's collective defense tasks were introduced. During the Warsaw Summit of 2016, "Commitment to Enhance Resilience" was adopted by the Alliance.[28]

NATO's Civil Emergency Planning Committee (CEPC) is involved in resilient building activities. CEPC contributes to NATO's strategic objectives with civilian expertise and capabilities in various fields such as terrorism, humanitarian aid, and disaster response, critical infrastructure protection, cyber and hybrid threats.[29]

[26] Ibid.
[27]Available at: http://www.nato.int/cps/on/natohq/topics_119353.htm
[28] Available at: http://www.nato.int/cps/eu/natohq/official_texts_133180.htm?selectedLocale=en
[29] Available at: http://www.nato.int/cps/on/natohq/topics_50093.htm

EU

In response to the needs of people with regards to their protection and improvement of livelihoods in current risk environment, European Union launches and funds several initiatives on sustainable development, disaster risk reduction, humanitarian assistance, climate change adaptation, and nutrition/food security.[30] Furthermore, due to rapidly increasing contemporary challenges posed by hybrid and cyber threats, EU expanded cooperation with NATO on enhancing resilience towards those threats.[31] The Directorate-General for European Civil Protection and Humanitarian Aid Operations of European Commission is the main contributor for maintaining and building resilience.[32]

UN

A number of entities of United Nations are involved in building and promoting resilience in various fields. This include resilience towards natural disasters (UNDP[33], FAO[34], ESCAP[35]), resilience of agriculture based livelihoods (FAO)[36], resilience of cities (UNISDR[37], UN-Habitat[38]), resilience in protracted crisis (FAO)[39], conflict prevention and peacebuilding (UNDP)[40], climate resilience (UN Secretary General's climate resilience initiative (A2R)[41] and many other short and long term initiatives.

What is NATO's approach to Resilience?

Seven baseline requirements;

- Assured continuity of government and critical government services;
- Resilient energy supplies;
- Ability to deal effectively with the uncontrolled movement of people;
- Resilient food and water resources;
- Ability to deal with mass casualties;
- Resilient communications systems;
- Resilient transportation systems. [42]

[30] EU(2016) Building Resilience: The EU's approach Factsheet
[31] NATO (2017): NATO - EU Relations – Fact Sheet
[32] Available at: http://ec.europa.eu/echo/what/humanitarian-aid/resilience_en
[33] Available at: http://www.undp.org/content/undp/en/home/climate-and-disaster-resilience/disaster-risk-reduction.html
[34] Available at: http://www.fao.org/resilience/areas-of-work/natural-hazards/en/
[35] Available at: http://www.unescap.org/our-work/ict-disaster-risk-reduction
[36] FAO (2016) Increasing resilience of agriculture based livelihoods
[37] Available at: https://unhabitat.org/urban-themes/resilience/
[38] Available at: https://www.unisdr.org/we/campaign/cities
[39] Available at: http://www.fao.org/resilience/resources/protracted-crisis/en/
[40] Available at: http://www.undp.org/content/undp/en/home/ourwork/democratic-governance-and-peacebuilding/conflict-prevention-and-peacebuilding.html
[41] Available at: http://www.a2rinitiative.org/
[42] Available at: http://www.nato.int/docu/review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm

NATOs´ approach on cyber-defense

In order to combat cyber threats it is noteworthy that NATO now recognizes cyber-space as a domain of operations as where they have to be as capable and effective as they are during air, sea and land operations. In pursuance of the prearranged aims NATO has released several projects and procedures to improve the allied cyber defense and to approach future cyber threats.

During the Wales summit in 2014 NATO members have agreed on passing a policy and action plan. This plan includes measures in order to establish and reinforce capabilities for cyber education and training. Furthermore, it enhances the information exchange between member countries and countries that might not be a part of NATO. Due to the asymmetric effects of cyber threats, the policy and action plan also comprehends internationally valid laws which are applying in cyber-space. On behalf of cyber defense, all member states have affirmed this law and included it into their national statutes.[43]

Another aspect is the integration of cyber-defense into NATO´s smart defense initiative. Hereby member states contribute resources and knowledge to form a joint task force. Especially the research and development department is in need of a lot of resources which most likely cannot be handled by a single country. Additionally, NATO has established a trust fund for cyber defense which can be used to finance the necessary activities and programs. Nameable projects are for example the Malware Information Platform (MISP) or the Multinational Cyber Defense Crisis Management Exercise (MN CD2).[44]

Because of the crucial prominence of the private IT-sector NATO has also started to cooperate with globally acting companies. By foundation of cross-sectional and multinational Smart Defense Projects, cooperating with private companies, both sides can profit from each other. Main goal is the exchange of expertise and technological innovations from either the military or private sector.[45]

NATOs´ approach to hybrid threats

NATO issued the Lisbon Summit Declaration in 2010, in which it explains how NATO is planning on tackling hybrid threats. Main aim is to defend its members against the full range of threats and to promote international stability. To stay effective over a long-term period, NATO members decided to operate more agile, cost-effective and to serve as an essential instrument for peace.

In pursuance of those goals, NATO is required to closer cooperate with political or military organizations such as the *European Union* or the *United Nations*. Besides working with allied countries it is also beneficial to deepen the relationship with non-allied but still influential powers like Russia. This cooperation might involve the exchange of inventories or information.[46]

[43] **NATO (2017):** Cyber defense, Online on the internet: URL: http://www.nato.int/cps/en/natohq/topics_78170.html.

[44] **Stoltenberg, J. (2017):** Press conference ahead of the meeting of NATO Defense Ministers, Online on the Internet: URL: http://www.nato.int/cps/en/natohq/opinions_145415.htm?selectedLocale=en.

[45] **NATO (2017):** NATO Policy on Cyber Defense, Online on the Internet: URL: http://www.nato.int/cps/en/natohq/topics_78170.html.

[46] **Bachmann, S.** (2012): *Hybrid threats, cyber warfare and NATO´s comprehensive approach for countering 21st century threats – mapping the new frontier of global risk and security management;* **in:** *Amicus curiae,* Vol. 8, 2012, P. 14-17.

NATO members agreed on developing new high-tech weapons systems (e.g. missile-defense), in the interest of protecting Allied countries against foreign or domestic attacks. With regard to not act aggressively towards surrounding countries, NATO officials have invited Russia to join the development process and planning.[47]

Beneficial to a successful long-term functionality it is also essential to enhance existing partner relationships and to develop and negotiate new ones with interested partners.[48]

Cooperation with partner countries

In the interest of resilience NATO has to go beyond the usual work within member countries. It is also important to establish long-term associations with neighboring countries or even partners from all around the globe.

Therefore, NATO has introduced several cooperating relationships which can contribute to fulfill the main goals, defined by the *United Nations Security Council Resolution*. These goals involve the protection and improvement of women rights, boarder defense and combating human traffic plus terrorism.

NATO has tight relations to the *Euro-Atlantic-Partners* (EAPC), which is a group of 29 Allies but also 21 non-member countries. Main task here is the consultation about political and security related issues, which include crisis management and peace supporting operations.[49]

Furthermore, NATO came up with the *Mediterranean Dialogue* Program, which was initiated in 1994. Hereby the 29 member states get the chance to step into contact with ambassadors of seven North-African states. Each state has the chance to consult collectively or individually with NATO in order to contribute to regional security and stability, to achieve improved mutual understanding and finally to dispel misconceptions about NATO among Mediterranean nations.[50]

While most current conflicts are located in the Middle East, NATO started the *Istanbul Cooperation Initiative (ICI).* The main reason behind it was to establish a security cooperation with such nations from the Middle East. It turned out to be a very helpful source contributing to regional and global security.[51]

Since security challenges are issues all around the world, NATO also tries to cooperate with partners around the globe. Therefore, they have established bilateral relations with countries who are not NATO or EAPC members.
In most cases those partners support NATO missions in either a military or civil way.[52] [53]

[47] **NATO** (2010): *Lisbon Summit Declaration*
[48] **Ibid.**
[49] **NATO** (2017): *Euro-Atlantic Partnership Council,* Online on the Internet: URL: http://www.nato.int/cps/de/natohq/topics_49276.htm
[50] **NATO** (2017): *NATO Mediterranean Dialogue,* Online on the Internet: URL: http://www.nato.int/cps/en/natohq/topics_60021.htm?
[51] **NATO (2017):** Relations with partners across the globe, Online on the Internet: URL: http://www.nato.int/cps/cs/natohq/topics_49188.htm?selectedLocale=en
[52] **NATO (2017):** NATO member and partner countries, Online on the Internet: URL: http://www.nato.int/cps/is/natohq/topics_81136.htm
[53] **NATO (2015):** PARTNERS, Online on the Internet: URL: http://www.nato.int/cps/cs/natohq/51288.htm

NATOs´ cooperation with the EU

The European Union and NATO are strategic partners. They cooperate on a wide variety of issues, including crisis management, capability development, building the capacities of partners, addressing hybrid threats and maritime security.[54] [55]

In July 2016, NATO and the EU expanded their relationship. As a result, a Joint Declaration was signed to boost cooperation in key, including countering hybrid and cyber threats, supporting partners in defense capacity building, improving information-sharing and cooperation in the Mediterranean Sea, as well as on defense capabilities, the defense industry and research, and exercises.

Following this a package of measures for the implementation of the Joint Declaration was presented in December 2016. These measures are now being implemented. They include: Measures to bolster resilience to hybrid threats, ranging from disinformation campaigns to acute crises, Enhanced cooperation between NATO's Operation Sea Guardian and the EUNAVFOR Operation Sophia in the Mediterranean Sea, exchange of information on cyber threats and the sharing of best practices on cyber security. Ensuring the coherence and complementarities of each other's defense planning processes as well as parallel and coordinated exercises, starting with a pilot project in 2017.[56] [57]

Close cooperation between NATO and the EU is an important element in the development of an international "Comprehensive Approach" to crisis management and operations but not new. NATO and the EU cooperate for years on crisis management and operations, in particular in the Western Balkans and Afghanistan. NATO and the EU worked and still work together in Bosnia and Herzegovina (SFOR/Operation EUFOR Althea), Kosovo (KFOR/EULEX), Afghanistan (ISAF/EUPOL), Coast of Somalia (Operation Ocean Shield/EUNAVFOR Atalanta), during the refugee crisis and in many more cases.[58]

[54] **Đajić, O. (2015):** The state of play of the EU – NATO partnership, Online on the Internet: URL: http://www.europeanleadershipnetwork.org/the-state-of-play-of-the-eunato-partnership_3076.html
[55] **NATO (2017):** NATO - EU Relations – Fact Sheet, Online on the Internet: URL: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170213_1702-factsheet-nato-eu-en.pdf
[56] Ibid
[57] **Pop, A. (2007):** NATO and the European Union: Cooperation and security, Online on the Internet: URL: http://www.nato.int/docu/review/2007/Partnerships_Old_New/NATO_EU_cooperation_security/EN/index.htm
[58] **NATO (2017):** NATO - EU Relations – Fact Sheet, Online on the Internet: URL: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170213_1702-factsheet-nato-eu-en.pdf

NATOs´ approach on civil-military readiness

NATO approaches civil-military readiness with its Readiness Action Plan (RAP) which was approved at the NATO Wales Summit in 2014. The RAP ensures that the Alliance is ready to respond swiftly and firmly to new security challenges. Due to that NATO members have to adjust their territorial defense mechanisms and infrastructure to the new security environment. This includes cross-border transit arrangements for the rapid deployments and the planning of transport, flight corridors, civil-military airspace coordination, fuel stocks, pre-positioned equipment, port access and legal agreements. Furthermore, the Allies have to update crisis-response, civil emergency and civil defense measures. These measures are the most significant reinforcement of NATO's collective defense since the end of the Cold War.[59]

Assurance measures - NATO's assurance measures are land, sea and air activities in and around NATO's territory, especially the eastern flank for reinforcing NATO's defense, reassuring civilians and deter aggressions. These measures are consequences of Russia's aggressive acts in the past. All Allies support these measures rotationally. The measures are flexible and annually reviewed by the North Atlantic Council. Examples for assurance measures are air-policing patrols, AWACS surveillance flights, maritime patrol aircraft flights, a Standing NATO Mine Counter-Measures Group and an enlarged Standing NATO Maritime Group. Furthermore, NATO has increased the number of exercises on land, at sea and in the air which improves the ability of Allies and partners to work together and is a demonstration of NATO's readiness and strength.[60]

Adaption measures - Adaption measures are long-term changes to allow the Alliance to react swiftly and decisively to sudden crises which include the tripling of NRF's strength, the creation of a Very high readiness Joint task Force (VJTF), the establishing of high-readiness multinational headquarters and enhancing Standing Naval Forces.

Enhanced NATO Response Force *(NRF)* - The NRF is a highly ready multinational force of land, air, maritime and Special Operation Forces (SOF) components. The NRF is quickly deployable. In 2014 the Allied countries decided, that the NRF should be enhanced to strengthen the collective defense. Since then the NRF has a size of approx. 40,000 personnel which is much larger than the old size of 13,000.

Very High Readiness Joint Task Force *(VJTF)* The VJTF, also called NATO's "spearhead force" has a size of approx. 20,000, of which about 5,000 are ground troops and is deployable within two or three days. The VJTF is supported by maritime and air components as well as SOF. VJTF forces are based in their home countries and will be deployed if needed. The command and membership of VJTF rotate every year.

NATO Force Integration Units *(NFIUs)* - NFIUs are small HQs which enable the deployment of the VJTF and other forces. They consist out of about 40 national and multinational NATO specialists. The task of the NFIUs is the improvement of the cooperation and coordination between NATO and national forces as well as to support and prepare exercises and deployments.[61]

[59] **Shea, J. (2016):** Resilience: a core element of collective defense, Online on the Internet: URL: http://www.nato.int/docu/review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm
[60] **NATO (2016):** NATO's Readiness Action Plan – Fact Sheet, Online on the Internet: URL: http://nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-rap-en.pdf.
[61] Ibid