Information & Security: An International Journal

Orlin Nikolov, v.39:1, 2018, 91-109 https://doi.org/10.11610/isij.3908

BUILDING SOCIETAL RESILIENCE AGAINST HYBRID THREATS

Orlin NIKOLOV

Abstract: This article addresses the efforts of NATO to improve societal resilience in the fight against hybrid threats. It examines hybrid threats as a military strategy that blends conventional warfare, irregular warfare and cyber warfare. From another point of view, the article sees over establishing a safe and secure environment for protection of civilians, as well as how to improve resilience through civil preparedness and tailored NATO support to national authorities. NATO requires a concept to be developed that operationalizes the NATO Policy with emphasis on its implementation through the planning and conduct of operations, training, education and exercises, lessons learned, as well as defence related capacity building activities. The article tackles the question of using the Centres of Excellence as an education and training network in building resilience in society against threats, including hybrid threats and protection of civilians.

Keywords: Hybrid threats, Protection of Civilians, Societal resilience, Crisis Management, Disaster response, Comprehensive Approach, Civil-Military Interoperability, Interagency cooperation, Risk reduction. Technical architecture, Centre of Excellence.

Introduction

In terms of awareness, NATO is concentrated in gaining appropriate military capabilities[1] at the expense of other instruments of power which are not developed in the field of economy and diplomacy. In order to have other instruments of power at its disposal which are crucial for countering hybrid threats, NATO has to establish relations and a level of coherence with other actors such as the EU. In order to counter *hybrid threats,* the security should be perceived as a broad concept, because these threats endanger the integral security of the whole society. Therefore, in countering it, all relevant actors should be engaged, thereby enhancing the process of transformation of NATO (including COEs). This will lead to a stronger political position, a clear strategical direction, and availability of the necessary ways and means.

Resilience is an essential basis for credible deterrence and effective fulfilment of the Alliance's core tasks. Under the North Atlantic Treaty, all Allies are committed to building resilience. In today's security environment, resilience more than ever requires a full range of capabilities, military and civilian, and active cooperation across governments and with the private sector. It also requires engagement with partner countries and other international bodies, and continuously updated situational awareness.

The hybrid threats predictably encompass a combination of full range of different modes including conventional capabilities, irregular tactics and formations, terrorist acts, including indiscriminate violence and coercion against civilians, and criminal disorder, which endangers the civilian population. In such a [dis]order, hybridized actors have the means to surprise and spread fear throughout the traditional nation-state community. These threats display different sorts of tactics, typical for asymmetric warfare and in particular for terrorism such as armed assaults against civilians, bombings (including suicide bombings) and explosions (including by using improvised explosive devices), assassinations, hostage taking of civilians such as kidnapping and hijacking. The violence included in hybrid threats is directed against civilian population. That is so because terrorism is a tactic in pursuit of political objectives, which necessitates the utilization of violence or the threat of violence against civilians. The use of violence against the civilians is rational, premeditated and has as a purpose the achievement of the ultimate objective, which at then is political. The motives can be different. The threat of using violence or the real use of violence is precise in terms of terrorist strategy and indiscriminate in terms of victims. Terrorists intend to produce extreme fear or terror and to exploit insecurity created by the fact that the population is in a continuous fear.

By reason of that, and for the purpose of building resilient society, the main priority of the international community and its main efforts should be directed against hybrid threats, and in particular terrorism which exploits the vulnerability of the democratic societies, and in particular of the individual, through spreading fear. The concentration on protection of civilians in times of hybrid threats is mandatory and a core business in the field of security.

NATO, through its network of centres of excellence, plays an important role in that respect:

> *NATO Centres of Excellence (COEs) Network* as nationally or multi-nationally funded institutions that train and educate leaders and specialists from NATO member and partner countries, should assist in building resilience in society against threats, including hybrid threats and protection of civilians.[2]

Until now, 24 NATO COEs are operational and we expect soon the 25th NATO COE for Foreign Fighters to be established. Most of them are connected in one, or more than one thematic area to provide subject matter expertise in their domain: Civil-

Military Cooperation COE, Combined Joint Operations from the Sea COE, NATO Command and Control Centre of Excellence, Cooperative Cyber Defence Centre of Excellence, Counter Improvised Explosive Devices (CIED) COE, Defence Against Terrorism (DAT) COE, NATO Energy Security Centre of Excellence, Explosive Ordnance Disposal (EOD), Human Intelligence (HUMINT) COE, Joint Chemical, Biological, Radiological, & Nuclear Defence (JCBRN), CMDR COE, Strategic Communications (STRATCOM) COE, and Stability Policing COE.

Resilience could be enhanced by exploring options in training requirements and activities, which would help develop a comparable level of expertise in critical areas.

Building Resilience in Society

Resilience is about achieving security and managing crises and cases of emergency. It is about the ability to protect population, buildings, systems, and networks. Building resilience is a challenging task in a globalized world, where new vulnerabilities and threats continuously emerge. It should be estimated as one of the core elements of the Alliance collective defence.

NATO strategic decisions at the Warsaw Summit defined a clear commitment to enhance resilience of Member States including by:

- re-affirming commitments under the North Atlantic Treaty;
- reaffirming the bond between Allies to defend one another against armed attacks;
- reaffirming the commitment to maintain and develop individual and collective capacity to resist armed attacks;
- stressing that the foundation for our resilience lies in a shared commitment to freedom, democracy, and the rule of law; and commit to uphold and defend these values;
- committing to improve resilience in five critical areas;
- maintaining and developing resilient and survivable military capabilities for credible deterrence and effective fulfilment of the Alliance’s core tasks;
- improving civil preparedness by meeting the seven baseline requirements for national resilience which focus on continuity of government; continuity of essential services and security of critical civilian infrastructure; and supporting military forces with civilian capabilities;
- further strengthening and improving the cyber defence of national infrastructure and networks in accordance with the separate Cyber Defence Pledge/ Commitment;

- improving the capabilities to prepare for, deter and defend against attacks using chemical, biological, radiological, or nuclear (CBRN) material;
- enhancing the supply chain security, focusing on multinational cooperation to enable the Allies concerned to sustain and eventually replace their Russian-sourced legacy equipment; and investment by the Allies concerned in replacement equipment;
- reaffirming the primary responsibility of nations to achieve resilience whilst stressing the need for coherent NATO support to assess and facilitate national progress.

The actions and commitments by the Allies and the other international bodies will also contribute to enhancing resilience, and stress that appropriate engagement is needed. Resilience is increasingly seen as the corollary of deterrence and reassurance measures in the classical military sphere as part of a comprehensive security strategy for the Alliance. The seven baseline requirements to be assessed are: 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 communication systems; and finally, resilient transportation systems. These seven areas apply to the entire crisis spectrum, from an evolving hybrid threat all the way up to the most demanding scenarios envisaged by Alliance planners.[3]

Therefore, to build resilience in society means to enable the public and the private sectors within given society in order to sustain resilience of infrastructures, supply and distribution systems, and cyber defence capabilities against hybrid threats and against all kinds of risks.

Building resilience has to encompass organizing cooperation between NATO bodies and COEs, the European Union Agency for Network and Information Security (ENISA), the European Institute for Security Studies, as well as protection of Critical infrastructures, energy networks, transport and supply chain, defence capabilities (cyber defence), public health and food security, and protection of civilians regardless of whether or not during armed conflicts or crises. It also includes action in terms of targeting hybrid threat financing and their sources including smuggling networks, non-governmental organizations, foreign states, transnational organized crime and transnational religious and ethnic fund-raising networks. The activities include managing networks and systems: removing illegal content and preventing radicalization and violent extremism, propaganda, recruitment, communication between terrorists, as well as reaction in terms of building mutual awareness in relation to crisis management procedures for reaction and resilience enhancement – close collaboration in strategic communication and cyber defence and joint exercises both at political and technical level with regard to decision making capacity.

Hybrid Threats

In the continuum of the conflict, the hybrid conflict is placed between a State conflict and a Non-State conflict. It blends conventional and irregular forces to create ambiguity, seize the initiative, and paralyze the adversary. It may include the use of both military and asymmetrical systems.[4] In terms of asymmetrical systems, NATO defines 'asymmetric threat/menace' as a threat "emanating from the potential use of dissimilar means or methods to circumvent or negate an opponent's strengths while exploiting his weaknesses to obtain a disproportionate result."[5]

In terms of capabilities, they are 'custom-designed' capabilities crafted by a principal actor to overcome the predominant power or position of an adversary.[6] These capabilities are designed to achieve the objectives of the principal actor. They are similar to the irregular tactics and unconventional warfare in the probability of targeting a wide range of military and civilian targets, including the population of the adversary. They are undertaken not to enhance the power of the attacker but to weaken the defender's power, position or influence. Hybrid threats are unique in terms of their ultimate objective. The objective is achieved not only by the *endogenous* capabilities of the actor but *exogenous* entities (agents), found by the actor, and are also included to supplement the capabilities and efforts of the actor. The relation between the actor (and its endogenous capabilities) and the agent (and its exogenous capabilities) is what matters regarding hybrid threats and their realization. Both are directed against the defender and are aiming at weakening or adversely changing its vital elements or instruments of power.

Hybrid wars "incorporate a range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder."[7] The multi-modal activities "can be conducted by separate units, or even by the same unit, but are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects in the physical and psychological dimensions of conflict."[8] Hybridity from this point of view is characterized by the interpenetration of a wide range of non-State actors (agents) including any combination of insurgent or terrorist networks, organized crime groups (sometimes with a nexus between the former and the latter), social groups such as clans, tribes, etc., ideologically or religiously motivated groups, and so on.

Hybrid warfare aims to keep the defender off the balance between its core elements—political, military, and societal—in order to control the situation and decide the direction of a crisis for the principal actor's benefit. NATO has several tasks in the face of hybrid threats – prevention or deterrence, defence or offence, and crisis management:

- Deterrence of principal actors that potentially intend to resort to hybrid warfare, subsequently prevention of any hybrid threat that, due to the intention and the realization, might emerge thereof;
- Defence against hybrid warfare by actors that cannot be deterred, subsequently an offensive response against a hybrid threat;
- De-escalation and mitigation of crises that have emerged due to hybrid threats or warfare.

In order to fulfil its tasks, NATO has to be *credible* to deter and prevent, *capable* to defend and act, and *efficient* in crisis management. This can be achieved through awareness, availability, and apparent preparedness.[9]

Coherence can be understood as "a scale of relationship that can be achieved [and that] depend[s] on the exact constellation of organizations in an interdependent relationship in that specific operational context."[10] Operations against hybrid threats, in order to be successful, depend on coherence. The concept aims at achieving "greater harmonization and synchronization among the activities of the international and local actors."[11] By achieving a level of coherence, it is possible to avoid the confrontation between military and political logic, turning both into a recognizable pattern of logical activity which supplement each other. Coordination is the process or the mechanism of interaction between actors which share a common perception, strategic vision and common objective to be achieved. Therefore, in the core, is the common objective which assumes a common strategy which leads to necessity for cooperation reflecting a level of coherence based on constellation.

Availability is crucial as we speak about enabling NATO's capabilities. It encompasses the classical conventional capabilities against conventional threats, including rapidly deployable intervention force, intelligence capabilities, Special Forces, nuclear capability, and capabilities related to cyber, information operations, strategic communication, leadership engagement, and psychological warfare.

The apparent *preparedness* will only be possible if the aforementioned elements are taken into account. Thereby, NATO has to enable all of its capabilities in a range of exercises in order to prepare. This includes the less classical capabilities (cyber, information operations, strategic communication, psychological operations) on which an emphasis should be put because they will be the key to success against hybrid threats. For the organization and realization of exercises and the contribution to a better preparedness of NATO, all relevant and competent actors have to be involved, including the Centres of Excellence. NATO has to improve its intelligence-sharing and early warning processes in order to better anticipate and map hybrid warfare activities. This involves:

- rapid identification of a hybrid attack;
- rapid decision making;
- effective strategic communication to dispel false information, propaganda, lies and myths.

Protection of Civilians (POC)

'Protection of civilians' is a framework meant to enhance the protection of civilian population from the effects of armed conflicts. According to the UN concept, the POC refers to the measures that can be taken in order to protect the safety of civilians during times of war, which are rooted in obligations under the aforementioned five-point legal framework. States have the primary responsibility to protect and meet the needs of civilians during armed conflicts. Organized armed groups and non-State actors have the same responsibility, too, under the international humanitarian law (IHL).[12]

The UNSC resolutions and other activities cross a spectrum that encompasses: exhorting parties to a conflict to uphold their legal obligations; robust measures to pressure parties to do so; measures to hold parties to account for serious violations of IHL, as well as authorizing operations to provide greater physical protection to civilians under threat of violence. In its resolutions, statements and missions to conflict regions, the UNSC frequently calls upon parties to a conflict to observe IHL. It also imposes sanctions on those violating IHL. In extreme cases, it has authorized action to hold individuals accountable for serious violations of IHL (for example, in the cases of the former Yugoslavia and Rwanda for which the UNSC established criminal tribunals or referring to situations to the International Criminal Court). The UNSC uses its Chapter VII powers to impose arms embargoes and to authorize UN peace operations, regional organizations or groups of member states to use military force for the protection of civilians.

Responsibility to Protect (R2P) and POC both require states to uphold specific, pre-existing obligations under IHL, refugee law and human rights law. Furthermore, as explained in the 2007 UN Secretary General's report on the protection of civilians, in its "important affirmation of the primary responsibility of each State to protect its citizens and persons within its jurisdiction from genocide, war crimes, ethnic cleansing and crimes against humanity," R2P has advanced the "normative framework" of the protection of civilians.[13]

Although sharing many features, R2P is not synonymous with POC. R2P is only a part of the broader agenda of protecting civilians during armed conflict, as R2P is specifically concerned with the protection of populations from genocide, war crimes, ethnic cleansing and crimes against humanity – the gravest violations of international humanitarian law and human rights. The rights of populations caught up in warfare extend well beyond protection from mass atrocities. R2P is concerned with preventing and halting crimes against humanity, genocide and ethnic cleansing regardless of whether or not they take place in the context of an armed conflict. The two agendas overlap but each extends beyond the other.[14]

Crisis management as a broad concept should include the protection of the population during crisis (before during and after armed conflicts) and disaster (natural or man-made). Therefore, protection of civilians should be a priority regardless of whether or not there is an armed conflict. It has to be a priority in the event of nuclear attacks, too. Further, the concept of ‘Rights Up Front" from 2014 of the UN can be relevant concerning the protection of civilians and adherence to the human rights law. It finds applicability within the NATO system, too. A number of elements are intended to complement Member States' action to discharge their responsibilities regarding POC. The common theme of the actions is to place the protection of human rights and of people at the heart of NATO strategies and operational activities:

> Action 1: Integrating human rights into the lifeblood of the [NATO] so all staff understand their own and the Organization's human rights obligations.
>
> Action 2: Providing Member States with candid information with respect to peoples at risk of, or subject to, serious violations of human rights or humanitarian law.
>
> Action 3: Ensuring coherent strategies of action on the ground and leveraging the [NATO] System's capacities to respond in a concerted manner.
>
> Action 4: Clarifying and streamlining procedures at Headquarters to enhance communication with the field and to facilitate early, coordinated action.
>
> Action 5: Strengthening the [NATO]'s human rights capacity, particularly through better coordination of its human rights entities.
>
> Action 6: Developing a common [NATO] system for information management on serious violations of human rights and humanitarian law.[15]

This concept can be enhanced and updated to the needs of NATO concerning the protection of population/civilians.

A comprehensive strategy for protection of civilians should be incorporated within the grand strategy and overall mission implementation plan. It has to include: assessment of potential threats, assessment of the options for crisis response and risk mitigation, establishing cooperation, coherence, and coordination between the different relevant actors, and establishment of priorities, actions and clear roles and responsibilities of the relevant and competent actors.

The Relevance of NATO COEs

The Centres of Excellence (COEs) as nationally or multi-nationally funded institutions that train and educate leaders and specialists from NATO member and partner countries should assist in building resilience in society against threats, including hybrid threats and protection of civilians. In the next pages in short is shown how everyone Centre of Excellences could contribute to the NATO efforts in the areas mentioned above.

The Civil-Military Cooperation COE [16]

Internal cooperation is aimed to facilitate dialogue between NATO structures, encompassing COEs of NATO in particular (pertaining to the hybrid threats). External cooperation – to facilitate dialogue between NATO and other institutions, in the field of hybrid threats, in particular: The European Union Institute for Security Studies; the European Union Agency for Network and Information Security; and the European Cybercrime Centre.

Subsequently, the COE is designed for the establishment of a strong EU-NATO relationship with regard to hybrid threats: relation between military and non-military actors, based on a comprehensive approach, and inventive ways to link military capabilities amongst NATO member States with diplomatic, economic and informational efforts, and protection of civilians – necessity to create partnerships designed to protect civilians: internal partnerships and external partnerships – civil-military cooperation within NATO in order to coordinate actions, and cooperation with the UN and different NGO partners. The COE works to enhance civil-military cooperation for:

- building common principles for protection that assume partnership arrangements;
- cultural awareness, common goals, shared responsibility, consent, transparency and communication;
- building balance between military, political, and economic objectives with humanitarian imperatives;
- a necessity for partnerships and relations between the military role and the humanitarian work;
- building a common concept for ‘protection of civilians,’ ‘the rules of law,’ ‘responsibility’ and ‘powers’;
- building common principles and doctrine;

- facilitating constant communication through meetings, training, and exercises;
- facilitating a multi-lateral cooperation which seeks to undermine the transnational links that keep hybrid conflicts going;
- Civil-military preparedness by:
    - Crisis-response measures to activate civil emergency measures;
    - Civil defence requirements based on the military requirements for the Readiness Action Plan and associated capability packages for its deployment;
    - A more sustained dialogue between military commanders and national civil emergency authorities;
- The integrated military-civil partnership regarding the protection of civilians encompasses:
    - Common understanding of the national interest and the drives of conflict and instability;
    - Common understanding of the strategy;
    - Joint training for civilians and military components in the field of protection of civilians;
- Clear understanding of the roles and responsibilities of each component of Integrated reporting, monitoring and learning.

Combined Joint Operations from the Sea COE [17]

Combined Joint Operations from the Sea (CJOS) COE participates as a key contributor and observer in three focus areas of countering hybrid warfare, countering unmanned autonomous systems, as well as joint and combined operations in and from confined waters.

NATO Command and Control Centre of Excellence [18]

> *The exercise of authority by a properly designated commander over assigned and attached forces, performed through an arrangement of personnel, equipment, communications, facilities and procedures in the accomplishment of the mission.*

To link military capabilities with ongoing diplomatic, economic and informational efforts by innovation, the transformation can be successful through:

- building ‘Culture of Innovation’;
- building ‘Hybrid Mindset’;
- hybrid threats /capabilities or/ and recommendations /for/ innovation.

The Centre provides on Strategical level warfare – understanding strategic context. Operational level warfare – holistic approach to operations and embracing the natural complexity of the operational environment, including information operations.

Tactical level warfare – to improve military readiness, providing greater speed and agility in decision-making. By doing so, the focus is on potential opportunities (OODA loop applicability).

Cooperative Cyber Defence Centre of Excellence [19]

The aim of the Centre is to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation.

The main goals are to enhance the capability and security, concerning the protection against cyber threats through:

- reliability of information systems and networks;
- protection of critical information infrastructures – data exchange;
- protection of government operations, commerce, and emergency services;
- protection of telecommunications and information systems;
- building cyber defence capabilities;
- managing networks and systems;
- removing illegal content, preventing radicalization and violent extremism;
- preventing terrorists for using information systems and networks as a means of propaganda, recruitment, and communication.

The COE contributes to establishing a sustainable 'security threshold' in the face of uncertainty concerning the cyber threats and their future realization, as well as to building coherence between military doctrine concerning cyber operations and technological and market realities of interdependent, and networked world.

NATO commanders need the requisite tools and authorities to defend against advanced cyber-attacks and to operate across the cyber spectrum.

Another area of interest is the protection of civilians during cyber operations including the peacetime international law governing cyber operations and the international humanitarian law that applies during armed conflict involving cyber operations, in particular the rules applicable in jus in Bello (principles of distinction, proportionality, etc.).

Counter Improvised Explosive Devices (C-IED) COE [20]

The C-IED COE mission is to provide subject matter expertise in order to support the Alliance, its Partners, and the International Community in the fight against Improvised Explosive Devices (IED) and co-operate to increase security of Allied Nations and also all the troops deployed in theatres of operations, reducing or eliminating the threats from improvised explosive devices used or for use, in particular by terrorists or insurgents.

One of the aspects of hybridity is the phenomenon of terrorism, the innovation in armament and subsequent implementation of terrorist tactics such as bombing and explosions – the latter including IEDs, used to instil fear within the population. The COE has to cooperate with the EOD COE in order to build capabilities to protect and deter hybrid threats, in particular terrorist threats.

Defence Against Terrorism (DAT) COE [21]

In a hybrid threat scenario, the initiator employs simultaneously regular and irregular forces, including terrorist and criminal elements. Therefore, terrorism is a tactic for achieving political objective and a threat for the population. As a tactic, terrorism is the premeditated use of, or threat of, violence against civilian population in order to achieve a given political objective. As a threat, it is an element of hybridity and is directed against civilians with the aim of instilling fear. There are direct and indirect targets of terrorism. The DAT COE should, first and foremost, build capacity to prepare, predict, prevent and respond to terrorist activities. It has to develop measures in order to battle terrorism, including the targeting of terrorist financing, managing networks and systems in order to remove illegal content and prevent radicalization and violent extremism. The COE should concentrate in building capacity for protection of critical infrastructures against terrorist threats and protection of cyber space, and taking the initiative and reducing the chances of terrorist activity in cyber space.

Cyber space is another terrain of conflict exploited by terrorists for propaganda, recruitment and communication. Measures of prevention should be constructed in order to halt the terrorist activity is cyber space. Measures particularly directed against the different strategies (attrition, intimidation, provocation, spoiling, lone-wolf, etc.) and tactics (armed assaults, unarmed assaults, bombings, explosions, assassination, hostage taking, facility attacks) of terrorists have to be developed. The defence of critical infrastructure in both the cyber and the physical space has to be developed against terrorist threats. As to the structures of the organizations of terrorists, the hybridity of the organizations has to be taken into account. A deep and detailed understanding of the operational and security capacity of the different types of terrorist organization is important in order to combat them with effective means. Hybrid threats including terrorism as a tactic applied by different terrorists organized in hybrid structures (can elaborate later on). Last but not least, mechanisms for re-action in cases of post-terrorism-situations wherein terrorist acts had emerged should be developed, i.e. building resilience in society as a capacity of individuals and the community as a whole to survive, adapt and grow in the face of stress and shocks, and to transform in events driven by terrorism and terrorist activity. Building resilience against post-terrorist-acts is about making population better prepared to withstand these terrorist events.

NATO Energy Security Centre of Excellence [22]

The Doctrine & Concept Development Division of the NATO Energy Security Centre of Excellence (ENSEC COE) is to provide Subject matter expertise in the field of energy security in order to support the transformational and operational requests of the Strategic Commands, the Sponsoring Nations and other Customers. This includes the contribution to the development of energy security related doctrines and standards.

The relevance of this COE can be seen from the *perspective of building resilience in society*. One of the main elements for achieving a sort of resilience is the protection of critical infrastructures and obtaining defence capabilities. The former is of vital importance. NATO has a specific approach concerning the field of energy security. NATO received a mandate to develop energy security related activities such as:

- information and intelligence fusion and sharing;
- projecting stability;
- advancing international and regional cooperation;
- supporting consequence management;
- supporting the protection of critical energy infrastructure.

NATO has to develop the capacity to contribute to energy security, including protection of critical energy infrastructure, transit areas and lanes. This capacity should include cooperation with Partners and consultation amongst Allies regarding strategic assessments and contingency planning.

Challenges in the field of energy security cannot be fully understood and analysed without taking into account other new security challenges such as cyber threats, terrorism or piracy. All three of these examples are transnational and can no longer be considered a matter of one individual nation’s security. Accordingly, the area of energy security has been identified as one of the most important capability shortfalls that constrain the Alliance’s mission effectiveness and interoperability in the area of countering hybrid threats and undermines NATO’s contribution to a comprehensive approach.

The protection of critical energy infrastructure is a must in times of globalization and hybrid threat challenges. Last but not least, efforts to protect energy infrastructure should be developed not only in the physical space (and against threats such as terrorism) but also in cyber space (against adversary cyber operations). By reason of the aforementioned, the NATO Energy Security COE should work in cooperation with other COEs, and in its field of competency (energy) in order to develop and sustain stability and security against hybrid threats.

Explosive Ordnance Disposal (EOD) COE [23]

The EOD COE focuses on terrorism, including as an element of hybridity and hybrid threats. It analyses terrorism strategies, terrorism tactics and use of explosives. In addition, it covers topics such as: Building resilience in society; PoC; Prepare, predict, prevent and respond to terrorist activities; Facilitate and support the full spectrum of Alliance operations. There is strong cooperation established with the IED COE and DAT COE concerning the threats emanating from terrorism.

Human Intelligence (HUMINT) COE [24]

Human intelligence as a means, utilized to combat hybrid threats, is of crucial importance. It is important for:

- locating sources and subsequent targeting of hybrid threat financing, including:
    - terrorism and guerrilla financing by smuggling networks; NGOs; foreign states; non-state actors; transnational organized crimes and transnational religious and ethnic fund-raising networks;
- locating and subsequent targeting of the relationship/nexus between principal actors and agents using offensive hybrid operations;
- locating and destroying the nexus between transnational terrorism and transnational organized crime;
- neutralizing different agents such as non-state actors;
- insurgent and terrorist networks;
- organized crime groups;
- social groups as clans, tribes, religious or ideologically motivated organizations, etc.

Joint Chemical, Biological, Radiological, & Nuclear Defence (JCBRN) [25]

Hybrid threats and offensive actions might cause conflicts and crisis. Chemical, biological, radiological and nuclear agents might be introduced in these conflicts. The prevention of acquiring that kind of capabilities from rogue States and terrorist organizations is of crucial importance for the whole world society well-being and its security. Weapons of Mass Destruction (WMD) might be a part of hybrid threats and warfare. These facts should not be excluded. On the contrary, they should be seriously taken into account. There are no limits for transnational organized crime and terrorism. Definitely, terrorist organizations and rogue States will try to obtain WMD.

Risks and threats should be assessed in regard to this. NATO credibility in terms of *prevention* and *deterrence* is a priority in this regard. NATO capability in terms of defence is also important.

Crisis Management and Disaster Response COE (CMDR COE) [26]

Crisis Management and Disaster Response (CMDR) COE is important in terms of building resilience in society. Decision-making is at the core of managing crisis and responding to hybrid threats and provocations. Therefore, joint exercises both at political and technical level with regard to decision-making capacity and efficiency should be conducted. This COE should work and support the three core elements and objectives of NATO – awareness, availability and preparedness, as we address hybrid threats and the best way to combat them. Expertise is important for NATO credibility and capability. NATO has to improve its intelligence-sharing and early warning processes in order to better anticipate and map hybrid warfare activities. This involves:

- rapid identification of a hybrid attack;
- rapid decision making;
- effective strategic communications to dispel false information, propaganda, lies and myths,

because hybrid conflicts serve to increase ambiguity, complicate decision making, and slow the coordination of effective responses against these threats. A capacity to overcome these issues needs to be developed.

Strategic Communications (STRATCOM) COE [27]

Strategic communications are an integral part of our efforts to achieve the Alliance's political and military objectives.

The current information environment, characterized by a 24/7 news cycle, the rise of social networking sites, and the interconnectedness of audiences in and beyond NATO nations territory, directly affects how NATO actions are perceived by key audiences. That perception is always relevant to—and can have a direct effect on—the success of NATO operations and policies. NATO must use various channels, including the traditional media, internet-based media and public engagement, *to build awareness, understanding, and support for its decisions and operations*. This requires a coherent institutional approach, coordination of effort with NATO nations and between all relevant actors, and consistency with agreed NATO policies, procedures and principles.

NATO Strategic Communication is the coordinated and appropriate use of NATO communication activities and capabilities in support of Alliance policies, operations and activities, and in order to advance NATO aims. These activities and capabilities are related first to Public Diplomacy which includes:

- promoting awareness of and building understanding and support for NATO policies, operations and activities;
- building credibility for deterrence and prevention of hybrid threats;
- establishing a strategy – building a nexus between military activities and political objectives concerning hybrid threats;
- building a balance between military, political, and economic objectives with humanitarian imperatives.

Hybrid threats cannot be effectively incapacitated and degraded only with conventional means. Building capacity in the field of diplomacy is important as generating means in the field of cooperation will be of crucial importance against hybridity. Therefore, the key to success is to define clear objectives built on clear strategies with regard to hybrid warfare, as well as building resilience and stability within a given society. In addition, it is important to establish close collaboration in strategic communication and cyber defence.

The second area of activity of the COE is related to Public Affairs which includes NATO civilian engagement through the media to inform the public of NATO policies, operations and activities against hybrid threats in a timely, accurate, responsive, and proactive manner.

The third area of activities covers Military Public Affairs, i.e. Promoting NATO military aims and objectives to audiences in order to enhance awareness and understanding of military aspects of the Alliance concerning the counter-actions against hybrid threats.

Finally, the fourth area covers Information Operations, or NATO military advice and co-ordination of military information activities in order to create desired effects on the will, understanding, and capabilities of adversaries and other NATO-approved parties in support of Alliance operations, missions and objectives.

The diplomacy is the key element and the key means to re-act against hybrid threats.

Conclusion

Societal resilience in NATO nations can be strengthened *inter alia* by close cooperation among the NATO centres of excellence. The idea is to bring together academic, operational and political expertise to integrate all E&T requirements and relationship with the target audience within NATO and Nations through several workshops.

This integrated programme may group, by modules, similar requirements for several audiences. The aim will be to describe the envisaged behaviour after training through learning objectives and depth of knowledge that the relevant training audience needs to receive. It will support the training providers with the learning outcomes to apply consistently for all the training activities.

The aim will be fulfilled through education and training activities, such as courses, workshops, seminars, trainings and exercises, etc. It could serve as the minimum military training requirements to enhance societal resilience posed by emerging treats.

The output will be to develop Program of Instruction (POI) combining all areas critical for societal resilience. The POI will combine a curriculum component (what we teach), and a teaching procedure (how we teach).

As an outcome, military and civilian personnel will be trained to be capable to engage in a timely and appropriate manner against the multiple challenges that have the potential to affect the security of the Alliance before they escalate into conflict.

Notes

[1] "Readiness Action Plan," *NATO Topics*, last updated September 21, 2017, accessed April 5, 2018, http://www.nato.int/cps/en/natohq/topics_119353.htm.

[2] Allied Command Transformation, "Centres of Excellence," accessed April 5, 2018, http://www.act.nato.int/centres-of-excellence.

[3] Jamie Shea, "Resilience: A Core Element of Collective Defence," *NATO Review* (2016), accessed April 5, 2018, https://www.nato.int/docu/review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm.

[4] David L. Raugh, "Is the Hybrid Threat a True Threat?" *Journal of Strategic Security* 9, no. 2 (Summer 2016): 1-13, quote on p. 6, https://doi.org/10.5038/1944-0472.9.2.1507.

[5] *NATO Glossary of Terms and Definitions AAP-06*, Edition 2014. The term has been added in October 2003.

[6] Frank J. Cilluffo and Joseph R. Clark, "Thinking About Strategic Hybrid Threats – In Theory and in Practice," *PRISM* 4, no. 1 (2014): 47-63, www.hsdl.org/?view&did=727928; "Countering Hybrid Threats: Challenges for the West," *Strategic Comments* 20, no. 8 (2014), x-xii, https://doi.org/10.1080/13567888.2014.992189.

[7] Cilluffo and Clark, "Thinking About Strategic Hybrid Threats."

[8] Frank G. Hoffman, *Conflict in the 21st century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007), accessed April 5, 2018, http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

[9] Margriet Drent, Rob Hendriks, and Dick Zandee, *New Threats, New EU and NATO Responses*, Clingendael Report (Clingendael: Netherlands Institute of International

Relations, July 2015); Cedric de Coning and Karsten Friis, "Coherence and Coordination: The Limits of the Comprehensive Approach," *Journal of International Peacekeeping* 15, no. 1-2 (2011): 243–272, https://doi.org/10.1163/187541110X540553.

[10] De Coning and Friis, "Coherence and Coordination: The Limits of the Comprehensive Approach," p. 244.

[11] De Coning and Friis, "Coherence and Coordination: The Limits of the Comprehensive Approach," p. 246.

[12] The UN Refugee Agency (UNHCR), *The 1951 Refugee Convention and 1967 Protocol* (Geneva: Switzerland, UNHCR, September 2011).

[13] Gareth Evans, "R2P and RWP After Libya and Syria," Keynote Address to the GCR2P/ FGV/ Stanley Foundation Workshop "Responsibility While Protecting: What's Next?" Global Centre for the Responsibility to Protect, August 2012, accessed April 5, 2018, http://www.globalr2p.org/publications/161.

[14] United Nations, 2005 World Summit Outcome, Resolution adopted by the General Assembly, Document A/RES/60/1, 24 October 2005.

[15] In December 2013, the UN Secretary General launched the Human Rights initiative called "Rights Up Front," which outlined these six actions intended to help the UN system meet its responsibilities regarding human rights.

[16] Civil-Military Cooperation Centre of Excellence (CCOE), http://www.cimic-coe.org.

[17] Combined Joint Operations from the Sea, Centre of Excellence (CJOS COE), http://www.cjoscoe.org.

[18] NATO Command and Control Centre of Excellence (C2COE), http://c2coe.org.

[19] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Tallinn, Estonia, https://ccdcoe.org.

[20] Counter Improvised Explosive Devices Centre of Excellence (C-IED COE), http://www.ciedcoe.org.

[21] Centre of Excellence Defence Against Terrorism (COE-DAT), http://www.coedat.nato.int.

[22] NATO Energy Security Centre of Excellence (ENSEC COE), https://enseccoe.org/en.

[23] Explosive Ordnance Disposal Centre of Excellence (EOD COE), www.eodcoe.org/en.

[24] NATO HUMINT Centre of Excellence (NATO HUMINT), http://www.natohcoe.org.

[25] JCBRN Defence Centre of Excellence, Vyškov, Czech Republic, http://www.jcbrncoe.cz.

[26] Crisis Management and Disaster Response Centre of Excellence (CMDR COE), https://www.cmdrcoe.org.

[27] NATO Strategic Communications Centre of Excellence (STRATCOM), Riga, Latvia, http://www.stratcomcoe.org.

About the Author

Col. **Orlin NIKOLOV** is Chief of Capabilities Branch, NATO's Crisis Management and Disaster Response Centre of Excellence, Sofia, Bulgaria. He graduated from Air force academy in 1991, and received a masters' degree from G.S. Rakovski National Defence College, Sofia. In 2017 he acquired PhD on National and International Security. He has authored articles and papers on air defence and modelling and simulations. Col. Nikolov has been leader and member of several NATO STO Modelling and Simulation Groups among which MSG 147 "M&S Support for Crisis and Disaster Management Processes and Climate Change Implications," MSG 134 "Distributed Simulation Architecture & Design, Compliance Testing and Certification" and MSG 106 "Enhanced CAX architecture, design and methodology." He has participated in national and international projects for Establishment and development of National Centre for Modelling and Simulation "Charalitza"; and Establishment and development of Integrated System for M&S in the Bulgarian MoD; He served as project manager for Establishment and development of Crisis Management and Disaster Response Centre of Excellence; Establishment of South Eastern Europe Education and Training Network; Investigating and assessing M&S Decision Making Support and Data Analysis platform for Crisis Management, Disaster Response (CMDR) and Climate Change, etc. *E-mail*: orlin.nikolov@cmdrcoe.org.