# THE SECURITY OF CRITICAL ENERGY INFRASTRUCTURE IN THE AGE OF MULTIPLE ATTACK VECTORS: NATO'S MULTI-FACETED APPROACH

**Amb. Dr. Sorin Dumitru Ducaru**[1]
NATO Assistant Secretary General, NATO
Brussels, Belgium
*ducaru.sorin@hq.nato.int*

**Abstract**
The current NATO threat landscape is characterized by a combination or "hybrid blend" of unconventional emerging challenges (like cyber and terrorist attacks) and re-emerging conventional ones (like Russia's recent military resurgence and assertiveness, that led to the illegal annexation of Crimea and destabilization in Eastern Ukraine). While the resurgence of the Russian military activity pushed the Alliance in the direction of re-discovering its deterrence and collective defence role, the new, not-traditional, trans-national and essentially non-military treats that generate effects below the threshold of an armed attack require a new paradigm shift with a focus on resilience although the protection of critical energy infrastructure is first and foremost a national responsibility, NATO can contribute to meeting the infrastructure protection challenge on many levels. Given the fact that its core deterrence and defence mandate relies in a great measure on the security of Allies' energy infrastructure NATO's role and

[1] Amb. Sorin Dumitru Ducaru is NATO Assistant Secretary General. As head of the Emerging Security Challenges Division which includes the Cyber Defence section he also chairs of NATO's Cyber Defence Committee (CDC) and the Cyber Defence Management Board (CDMB). The opinions are provided in this paper on personal, expert basis and should not be interpreted as engaging NATO.

actions in reducing the vulnerabilities and strengthening the resilience of such infrastructure can only increase. A multi-faceted, multi-stakeholder and networked approach is needed to be able to strengthen defences and resilience of critical infrastructure such as energy. Understanding and defending against cyber or terrorist threat vectors, increased situational awareness, education, training, exercises, trusted partnerships as well as increasing strategic security dialogue and cooperation are key for such a comprehensive/network approach to the challenge.

**Keywords**
Collective defence, deterrence, early warning, education, exercises, hybrid warfare, resilience, security of energy infrastructure, training, terrorism

## 1.INTRODUCTION: A DOUBLE PARADIGM SHIFT FOR NATO

Russia's illegal annexation of Crimea in 2014 is widely regarded as a paradigm shift for NATO. After a quarter century of focusing on crisis management operations, the transatlantic alliance was prompted to re-discover its traditional core mission of collective defence and deterrence. Accordingly, NATO has embarked on the biggest military reinforcement since the end of the Cold War. By establishing a military presence in Central and Eastern Europe, NATO brings home to Allies and adversaries alike that the military solidarity between the members of the Alliance is rock-solid.

Yet the return of collective defence is only half the story. Underneath the return to collective defence and deterrence lies a second paradigm shift that is still less clearly identified and acknowledged the growing importance of non-traditional, non-military threats against the infrastructure of modern industrial societies. As these threats cannot be deterred by traditional military means, they put the onus on enhancing "resilience". Only if both shifts are sufficiently understood will NATO be able to remain an effective provider of security for its 900 million citizens. Although many of these threats occur below the threshold of an armed

attack and therefore might not face the deterrent effect of a collective defence response under Article 5 of the Washington Treaty, they can, however have significant implications upon human, social, economic activity or upon national and international security.

How is NATO coping with the second part of this paradigm shift, namely enhancing resilience? This paper seeks to answer this question by looking at the challenge of protecting critical energy infrastructure through the prism of NATO's recent experience.[1] Although the protection of critical energy infrastructure is first and foremost a national responsibility, NATO can contribute to meeting the infrastructure protection challenge on many levels. Given the fact that its core deterrence and defence mandate relies in a great measure on the security of Allies' energy infrastructure NATO's role and actions in reducing the vulnerabilities and strengthening the resilience of such infrastructure can only increase. The recent implementation of the Alliance Enhanced and Tailored Forward Presence in the countries on the Eastern frontier of the Alliance can only underscore this aspect since mission success will depend on the reliability and resilience of critical infrastructure in the Allied host nations.

## 2.THE IMPORTANCE OF STRENGTHENED ENERGY INFRASTRUCTURE CYBER DEFENCES

Given its critical role in the functioning of a modern economy as well as in supporting collective defence efforts, energy infrastructure remains among the most critical components that determine a nation's security. Increasing digitisation (e.g. smart grids, smart meters and the internet) has made the energy sector more efficient, yet at the same time more vulnerable. For example, attacks

[1] NATO's role in Critical Infrastructure Protection in general does not rely on a regulatory approach. Rather, the focus is on building skills and capabilities, for example by promoting governance and resilience in the field of civil emergency planning with a focus on consequence management. The main goal is to support national plans by promoting higher standards of preparedness and better interoperability in consequence management.

on Industrial Control Systems can result in massive physical damage such as the breakdown of critical machinery, which cannot be replaced quickly. A well-orchestrated cyberattack could thus bring down crucial components of a country's energy infrastructure, resulting in massive economic and financial disruption and arguably even loss of life. Unsurprisingly, therefore, the energy sector is also among the targeted sectors by cyber attackers. According to the former Director of the US National Security Agency, General Keith Alexander, 41% of cyber-attacks are targeting energy enterprises, particularly oil and gas (Schouker 2016).

NATO has long recognised the increasing importance of cyber defence. While the major focus of NATO's effort is directed at protecting NATO's own networks, the magnitude of the cyber challenge requires much more than mere technical improvements. Consequently, NATO has developed a comprehensive cyber policy that brings together technical, political and legal elements. One visible step in this regard was the recognition of cyberattacks as a potential trigger for invoking Article 5 of the Washington Treaty, NATO's collective defence clause. NATO has also recognised cyber as a distinct military domain, on a par with land, sea and air.

NATO's Cyber Defence Policy also provides for streamlined cyber defence governance, procedures for assistance to Allied countries in response to cyberattacks, and the integration of cyber defence into operational planning, including civil emergency planning. Further, the policy defines ways to take awareness, education, training and exercise activities forward, and encourages further progress in various cooperation initiatives, including those with partner countries and international organisations. Cooperation with industry and other important actors, such as the European Union will allow further progress in minimizing vulnerabilities. Companies will also have to develop a better understanding of the need for investing in cyber defence, and not simply discard such financial investments as detrimental to one's competitiveness.

Another challenge is the cyber defence related training of energy infrastructure operators: the damage inflicted by the reckless handling of computers and storage media could be much reduced by greater awareness. In particular, the shift from information technology (IT), where the focus is on securing data, to

Industrial Control Systems (ICS), where the focus is on securing the operation, must be sufficiently understood by everyone involved. Consequently, NATO's work on cyber defence education and training, most prominently through its Centre of Excellence in Estonia, includes education on Critical Information Infrastructure Protection, where issues such as investment in protection, information sharing and risk assessment are being discussed.

In addition, energy systems in the military may also be vulnerable to cyberattacks. In particular, such vulnerabilities might exist in fuels distribution, which has become fully automatised. For example, the Pentagon has adopted networked computers for all dimensions of administrative and logistical activity, while the US Defense Logistics Agency (DLA) holds the mandate for fuels provision for the armed services and has developed digital tools to perform its fuels supply mission. Moreover, DoD fuels management utilises Windows-based client-server applications (Bronk 2014, 14). Thus, military energy systems are not immune to cyberattacks.

## 3.DEFENCE AGAINST TERRORISM

Most analysts agree that international terrorism represents the main man-made threat to energy infrastructure as long as it has effects over the human life. The low number of successful or attempted terrorist attacks against the energy infrastructure of NATO members may indicate that, at present, terrorist groups do not possess the resources or knowledge to conduct coordinated major attacks against energy infrastructure assets on NATO territory. According to some sources, three non-NATO countries – Colombia, Iraq and Pakistan – account for half of all attacks worldwide on energy infrastructure in the years 1980 – 2011 (Giroux, Burgherr, Melkunaite 2013). However, risks to critical energy infrastructures cannot be confined to specific borders. As NATO member states still heavily depend on energy imports from regions outside NATO, a terrorist attack on energy infrastructure facilities outside NATO member countries' borders can considerably reduce the Alliance's access to energy resources.

Moreover, some energy producing regions, especially in the Middle East and North Africa, are particularly vulnerable to threats against energy infrastructure and suffer from hundreds of terrorist attacks each year. Finally, the world's energy production industry is still very much concentrated in relatively few areas – for example, half of the world's oil production comes from just over 100 large oil fields. As the characteristics of the oil industry makes oil prices very sensitive to any kind of disturbance, even an unsuccessful attempt to target strategic energy facilities could cause major oil price hikes.

Over the years NATO has acquired valuable expertise in countering asymmetric threats and in responding to terrorism. Through the Defence Against Terrorism Programme of Work NATO works on capability development, the use of innovative technologies and improvements to procedures – this can cover topics as diverse as hardening of helicopters against shoulder-fired anti-aircraft missiles, to improved procedures for clearance of mines and Improvised Explosive Devices from convoy routes. These efforts are matched by work on preparedness to deal with the consequences of attacks – including the threat of Chemical, Biological, Radiological and Nuclear (CBRN) attacks – through civil emergency planning and training coupled with critical infrastructure protection. NATO's Centres of Excellence are important contributors to many projects, providing expertise across a range of topics including military engineering for route clearance, countering IEDs, explosives disposal, cultural familiarisation, network analysis and modelling.

While the protection of energy infrastructure is not in the centre of NATO's counterterrorism approach, the fact that terrorists often target such infrastructure is reflected in the efforts of the Alliance to raise awareness through education and training activities. NATO's Centre of Excellence on Counterterrorism in Turkey plays an important role in this regard, for example by offering courses that also cover Critical Infrastructure Protection. The NATO School in Oberammergau, Germany, is also integrating lectures on terrorist threats against critical energy infrastructure into relevant courses. NATO can also call on an extensive network of civil experts, from government and industry, to help respond to requests for assistance. Its Euro-Atlantic Disaster Response Coordination Centre (EADRCC) coordinates responses to national requests for

assistance following natural and man-made disasters including terrorist acts involving CBRN agents.

## 4.EDUCATION, TRAINING, AND EXERCISES

The growing importance of energy considerations in the international political debate is making energy security a permanent fixture in NATO's education and training programmes. Diplomats and military leaders alike must be given the opportunity to develop a better understanding of energy and related issues, such as resource competition and climate change, as drivers of future security developments. In addition, energy supply disruptions and critical energy infrastructure failures could affect not only the normal functioning of the economy, but also – as was clearly demonstrated in the case of Ukraine – a country's ability to effectively organise its defence. Energy is therefore a tempting target in hybrid warfare, and preparedness for energy-related incidents through training and exercises is key for a comprehensive defence.

To this end, new energy security courses have been set up at NATO's training facilities as well as the NATO Energy Security Centre of Excellence in Lithuania, and existing courses and exercises are augmented with appropriate energy-related elements. Given that NATO has no direct role in critical energy infrastructure protection, the focus of most such courses lies on strategic awareness, i.e. they provide the participants with a clearer understanding of threats to energy infrastructure. However, Table-Top Exercises (TTX), for example, also allow for a focused analysis of very specific infrastructure challenges. The NATO Energy Security Centre of Excellence, for example, has conducted such a TTX with Ukraine and even contributed to a "Green Book" about Ukraine's electricity network (Biriukov, Kondratov, Nasvit, Sukhodolia 2015).

The challenge of critical energy infrastructure protection will be increasingly reflected in NATO's exercises. The more non-traditional challenges such as energy and cyber are being incorporated in relevant exercise scenarios, the more the players will be forced to realise the criticality of energy supply, including for

military planning. Here, too, the Centres of Excellence have emerged as major enablers, due to their flexibility in organising and conducting a wide range of training and exercise events on energy infrastructure challenges.

## 5.INCREASED SITUATIONAL AWARENESS THROUGH INTELLIGENCE SHARING AND STRATEGIC ANALYSIS

By bringing together over 60 intelligence services, NATO provides a unique forum for discussing current and future threats, including to energy security. Intelligence-sharing includes the security of critical energy infrastructures, particularly in energy producing and transit countries; and the security of transport routes. To further enhance situational awareness, NATO has stood up an Intelligence Security Division in its International Staff. In addition, NATO has also expanded its in-house analytical capabilities, allowing for a more forward-looking analysis of how energy, economic, environmental and other factors may affect Allied interests and impact on NATO's policies and operations.

The crises to the East and to the South of NATO feature significant energy dimensions. To the East, Russia continues to use energy as part of its hybrid strategy of ensuring that its neighbours remain weak and fragile. To the South, the low oil price environment threatens to destabilise energy exporting states in Middle East and Northern Africa, which used to safeguard against domestic unrest through generous subsidies to their populations. In Syria and Northern Iraq, Daesh (ISIL) managed to fund its operations from illegal oil sales over a considerable period, making it the world's wealthiest terrorist organisation. All these developments require intensified intelligence sharing among Allies to allow for a comprehensive assessment of their numerous political, economic and military implications for Allies and the Alliance.

The need for better situational awareness is particularly important in an age of "hybrid" conflicts, where an opponent uses an array of non-military means to create the kind of ambiguity that could undermine a collective response by the Allies. For example, in order to de-stabilise Ukraine, Russia applied a

combination of military, semi-military and strategic communication tools. But it also managed to integrate energy (via the expropriation of Ukrainian energy assets and pressure on the gas prices) into this strategy. Hence, if NATO wants to be serious about effectively countering "hybrid threats", it must include energy into the equation.

## 6.THE ROLE OF TRUSTED PARTNERSHIPS

NATO's partnership network includes many energy producers and transit countries, some of which have expressed serious interest in working with NATO in the field of energy security. Consequently, sharing best practices on the protection of critical energy infrastructure remains NATO's most frequently offered cooperation item with respect to energy security. Activities in this regard benefit from NATO's longstanding expertise in crisis and consequence management and from the effective involvement of the private sector, whose unique expertise can be made available to partners through the NATO framework.

Given that the protection of critical energy infrastructure is a national responsibility, NATO's role is largely that of a facilitator. However, experience shows that it is the specific NATO context that attracts the attention of stakeholders, notably partner countries and industry. NATO's Science for Peace and Security Programme has also emerged as an effective tool to further developing practical cooperation with partners, as it provides opportunities for NATO member and partner countries to develop new methodologies and technologies in the field of energy security, including the protection of critical energy infrastructure.

In addition to regular meetings among Allies on energy security issues, individual partners can meet with Allies at various levels in the so-called "28+n" format. These meetings have given Allies detailed insights about these partners' energy policies and security perceptions. In turn, these partners were provided with a highly valued opportunity to inform Allies about their national energy

outlook and their expectations about future cooperation. Moreover, upon the request of a partner country and agreement by Allies, NATO can dispatch Advisory Support Teams (AST) to evaluate infrastructure vulnerabilities or assess damage to energy installations, as was the case in Georgia after the 2008 war with Russia. Similarly, after the outbreak of the Russia-Ukraine crisis in 2014 NATO dispatched an AST to Kiev to review the emergency plans of Ukrainian power plants. NATO also can, upon request, support the protection of partners' critical energy infrastructures, whether by supporting national communication and intelligence networks or through aerial and maritime patrols.[1]

## 7.OUTREACH TO OTHER INTERNATIONAL ORGANISATIONS AND THE PRIVATE SECTOR

When it comes to energy infrastructure protection, the logic of partnership extends far beyond individual nations. For example, most of the relevant energy data is being collected and analysed by specific institutions, notably the International Energy Agency (IEA). NATO cannot match, nor should it duplicate, the superb analytical resources of the IEA in the area of energy. However, NATO also cannot afford to miss important energy elements in assessing the wider security picture. Hence, the way forward lies in regular dialogue and mutual participation in certain exercises. This will contribute to a consistent evaluation of energy risks, including those with a hybrid dimension.
The logic of partnership also applies to NATO's relations with the European Union. Many of the new challenges are both internal and external in nature. For

[1] While the protection of land-based critical energy infrastructure is not a dedicated NATO responsibility, the maritime domain presents a different picture. Today about one-half of energy resources is moved by tankers on fixed maritime routes, which means that any NATO naval operation that contributes to the security of major sea lanes is, by definition, also a contribution to energy security. By protecting international shipping off the Horn of Africa, NATO's counter-piracy operations in the Indian Ocean have clearly demonstrated the potential to deter or disrupt actions that could undermine energy supplies. Accordingly, NATO's maritime strategy documents make a clear case for the role of navies in energy security.

example, terrorism can be home grown or imported, while protecting national networks and energy infrastructures are essentially national responsibilities. This poses entirely new coordination challenges for all actors involved. A stronger NATO–EU relationship would be a major step toward overcoming such challenges. Moreover, the Ukraine crisis demonstrated the EU's growing effectiveness as an energy actor. The Union's role in brokering a deal about the price of Russian gas for Ukraine, as well as its success in organising organizing the "reverse flow" of Russian gas to Ukraine via Poland and Slovakia, were impressive examples of an emerging European energy solidarity, in this case even for the benefit of a non-EU neighbour.

Against this background, NATO-EU discussions on hybrid threats, staff-to-staff collaboration, and the search for greater synergies in each other's training and education efforts appear both urgent and feasible. While Norway and Turkey remain outside the EU for the time being, their respective roles as an energy producer and energy hub for Europe would suggest that a NATO-EU dialogue is fully in line with their own security and economic interests. While certain national sensitivities of NATO Allies and EU members must be respected, the urgency for closer coordination and cooperation between both organizations is greater than ever.

Another part of a better connected NATO is a sustained relationship with the private sector. The reason for this is simple: most of the critical infrastructure is owned by private companies. According to the US Department of Homeland Security, 85 percent of the US critical infrastructure is owned by the private sector (*Critical Infrastructure protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics* 2016, 29). Hence, just as the urgency to enhance NATO's cyber defence capabilities will lead to closer ties with a range of companies, the need to develop a coherent approach to energy security will require NATO to reach out to private energy enterprises. Creating such new relationships will be challenging, since national business interests and collective security interests may sometimes prove to be irreconcilable. For example, companies may share a common interest to defend against cyberattacks, but they still remain competitors. Companies also need to balance their obligations to governments (i.e. reveal all data) with their obligations to

their customers (i.e. protect their privacy from government snooping). Still, the nature of many emerging security challenges makes the established compartmentalization of responsibilities between the public and private sectors appear increasingly anachronistic.

## 8.THE CRITICAL ROLE OF RESILIENCE

Armed forces today are more reliant than ever on infrastructure that is civilian-owned or operated. To have assured access to these capabilities, NATO requires robust civil preparedness in allied nations, across both the public and private sectors. Moreover, civilian services and infrastructure are potentially vulnerable to outside attack or internal disruption — and such vulnerabilities could be exploited by potential adversaries.

In the Cold War, NATO featured elaborate policies and planning for civil preparedness, involving more than 1,400 international civilian experts, as well as corresponding resources in all NATO members' capitals. The end of the Cold War led to a dramatic reduction of these capabilities. Only in 2014, when NATO's return to collective defence brought home the need to re-think civil preparedness, another systematic effort was undertaken to improve resilience across the Alliance. Based on an assessment of threats and vulnerabilities, Allies agreed on a set of minimum standards for national resilience, so-called "baseline requirements," in those areas that were deemed most critical to NATO's collective defence tasks, including resilient energy supplies.[1] These baseline

[1] 1. *Continuity of Government*: maintaining at all times the ability to make decisions, communicate them, and enforce them, and to provide essential government services to the population.
2. *Resilient Energy Supplies*: ensuring that energy supply, including national power grids, are secure and that nations maintain the necessary prioritization arrangements and redundancy.
3. *Resilient Civil Communications Services*: ensuring that telecommunications and cyber networks remain functional even in demanding conditions and under attacks.
4. *Resilient Food and Water Supply*: ensuring sufficient supplies are available to both civilians and the military, and safe from disruption of sabotage.
5. *Ability to Deal with Large Scale Population Movements* and to be able to de-conflict such movements from potential national or Alliance military deployments and other requirements.

requirements assist nations in conducting national self-assessments of their resilience. They are, in essence, a minimum standard. They represent the level of resilience that each Ally is expected to meet so that the core functions of continuity of government, continuity of essential services to the population and civil support to the military are at all times maintained – even in the most demanding scenarios.

The baseline requirement on resilient energy supplies aims at assuring access to reliable supply, including alternative sources of energy in the event of reduced availability and effective prioritisation arrangements. This requires robust and sustainable back-up plans and redundant power grids. Moreover, critical supply chains and interdependencies, in particular cross-border interconnections, need to be identified and prioritised. In other words, "resilience", including of energy systems, is now recognised as an essential basis for deterrence and the effective fulfilment of the Alliance's core tasks.

In order to be able to deter and defend against the full range of modern threats, allies need to maintain and protect critical civilian capabilities alongside and in support of military capabilities in an integrated way, and with the involvement of the whole of government and the private sector. Delivering the forces and other military capabilities that NATO requires to implement its collective defence mission or to project forces beyond its territory relies on civilian resources, including energy. During the Cold War, many of these resources, such as railways, ports, pipelines or electricity grids, were state-owned and thus could be easily transferred to NATO's control in crisis or wartime. Today, by contrast, 90 per cent of NATO's supplies and logistics are moved by private companies and 75 per cent of the host nation support for NATO forces forward deployed on the territory of the eastern Allies comes from private sector contracts (Shea 2016).

---

6. *Ability to Deal with Mass Casualties*: ensuring that health systems can cope even in very demanding situations when there might be simultaneous pressure on civilian and military health care capabilities.

7. *Resilient Civilian Transportation Systems*: ensuring that NATO forces can move across Alliance territory rapidly and that civilian transportation networks remain functional and effective to support civil and military requirements even when challenged or attacked.

Allies have also understood that, since resilience is first and foremost a national responsibility, nations must each develop and build systems that suit their own national circumstances. Finally, NATO's resilience can also be enhanced by the work of other organizations, in particular the European Union, and by strengthening the resilience of partner countries in the Alliance's neighbourhood.

## 9.A BROADER STRATEGIC SECURITY DIALOGUE

Further enhancing NATO's ability to meet non-traditional security challenges requires more than bureaucratic moves. It also requires a regular dialogue among Allies about broader security developments, including about challenges that are not military in nature. Thus far, many NATO members approach such discussions only hesitantly, worrying that NATO's image as a military, operations-driven organisation will unduly "militarise" non-military subjects. However, such a view risks holding NATO hostage to common misperceptions: the Allies would condemn themselves to an entirely reactive approach and thus forego opportunities for a pro-active policy.

Such a culture of forward-looking debate is all the more important as many new security challenges do not affect all Allies in quite the same way. A terrorist assault or a cyberattack against just one Ally will not necessarily generate the collective sense of moral outrage and political solidarity that one could witness after ''9/11.'' Consequently, political solidarity and collective responses may be far more difficult to generate than in the past. Admitting this is not fatalism. It is simply a reminder that the new threats can be divisive rather than unifying if allies do not make a determined effort to address them collectively. On a positive note, there are some indications that this cultural change in NATO has finally begun, as Allies have become more willing to discuss potentially controversial issues in a brainstorming mode. This welcome development must now be sustained, as pointed out above, by beefing up NATO's analytical capabilities, including improved intelligence sharing and longer-range forecasting.

## 10.CONCLUSION: "IT TAKES A NETWORK TO DEFEAT A NETWORK"

The double paradigm shift toward deterrence and defence as well as toward resilience constitutes an enormous challenge both for individual states as well as for alliances. A security policy that accepts that certain threats cannot be prevented through deterrence, and that some damage will thus inevitably occur, may appear to some as overly fatalistic or even outright scaremongering. Still, the governments of modern industrial societies have no choice but to admit to their citizens that in an era marked by energy vulnerabilities, terrorism and cyberattacks neither the individual state nor an alliance can still offer the near-perfect protection their populations may have enjoyed in earlier decades.

Governments will therefore have to develop new forms of protection and consequence management, yet without creating a climate of fear and uncertainty. This is challenging, but it can be done. While today's security environment may be more complex than ever before, the means to cope with it have also grown. Not only have individual actors, such as International Organisations, broadened their respective remit and range of instruments; they have also started to work together, in order to exploit synergies and minimise wasteful duplication. NATO's recent evolution is a case in point: in response to a changing security environment it has enhanced its deterrence and defence posture and put additional emphasis on enhancing the resilience of infrastructure. At the same time, however, it has intensified its outreach to other institutions as well as the private sector. In short, NATO is increasingly positioning itself as part of a much broader security network. This logic of networking along with the associated change of mind-set is the key to security in the 21st century.

## REFERENCES


- Schouker, P. "*The Energy Sector: A Prime Target for Cyber Attacks*", http://foreignpolicyblogs.com/2016/06/02/energy-sector-prime-target-cyber-attacks/, published on 2 June 2016.
- Speech by NATO Secretary General, Jens Stoltenberg at the Center for Strategic and International Studies (CSIS) in Washington D.C.: "Adapting to a changed security environment", 27 May 2015, http://www.hq.nato.int
- Ch. Bronk, *Hacks on Gas: "Energy, Cybersecurity and U.S. Defence"*, James Baker II Institute for Public Policy, Rice University, 2014, p. 14.
- J. Giroux, P. Burgherr, L. Melkunaite, "*Research Note on the Energy Infrastructure Attack Database (EIAD"*, Perspectives on Terrorism, Vol 7, No 6 (2013).
- Hannigan, Robert "The web is a terrorist's command-and-control network of choice", *Financial Times* 3 November 2014. Accessed on 15 October 2015. http://www.ft.com/intl/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3O7qCcpPj .
- Hoffman, F.G. "Hybrid Warfare and Challenges", *JFQ Joint Force Quarterly*, 2009.
- Jones, Sam "Ukraine: Russia's new art of war", *Financial Times*, 27 August 2014, accessed on 15 October 2015http://www.ft.com/intl/cms/s/2/ea5e82fa-2e0c-11e4-b760-00144feabdc0.html.
- D. Biriukov, S. Kondratov, O. Nasvit, O. Sukhodolia, *Green Paper for the Protection of Critical Infrastructure in Ukraine: Analytical Report*, National Institute for Strategic Studies, Kyiv, 2015.
- NATO Warsaw Summit Declaration, 09 july 2016, http://www.hq.nato.int.
- Speech by NATO Deputy Secretary General, Ambassador Alexander Vershbow at the Interparliamentary Conference on CFSP/CSDP, Riga, Latvia, 5 March 2015, accessed on 15 October 2015http://www.nato.int/cps/en/natohq/opinions_117919.htm.
- Statement by NATO Ministers of Defence, 25 June 2015, accessed on 11 October 2015, http://www.hq.nato.int.
- *Critical Infrastructure protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics*, US Government Accountability Office Report GAO-07-39, 16 October 2016, p. 29
- J. Shea, *Resilience: A Core Element of Collective Defence*, NATO Review, 30 March 2016.