THE CYBER DIMENSION OF MODERN HYBRID WARFARE AND ITS RELEVANCE FOR NATO

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

Abstract
The technological development and the instant communication possibilities advanced not only economic and social developments, but also evolving threats from those who exploit the vulnerabilities of communication and information systems. The cyber threat landscape points to a significant increase of the frequency, intensity, duration and sophistication of cyber-attacks. One of the new and concerning trends is the use of cyber capabilities in relation with military of hybrid operations – the so-called cyber dimension of hybrid warfare. NATO's strategy on countering hybrid warfare is based on the triad: prepare-deter-defend, which also applies to cyber. Nations represent the first line of defence in countering hybrid strategies. International cooperation is also a key factor in this sense. It is in this context that NATO's response to cyber-attacks in the context of hybrid warfare must be further refined.

Keywords
Cyber defence; information warfare; hybrid warfare; early warning; resilience; risk management

---

[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 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.

1. INTRODUCTION. THE FAST EVOLVING CYBER THREAT LANDSCAPE

A qualitative general description of the dynamics of the international cyber threat landscape points to a significant increase of the frequency/number, intensity, duration and sophistication of cyber-attacks, in particular over the time-span of the last year and a half. This trend that can be depicted at international level is consistent with threat assessments against NATO networks.

These aspects that are defining the qualitative evaluations of the evolving cyber threat landscape are supported by some notable insights from data collected by industry and reported recently. Some indicative examples are presented below:

a. Symantec noted in its 2015 Internet Security Threat Report (ISTR) that there were 314 million new pieces of malware created in 2014 alone (Symantec Internet Security Threat Report 2015); the same report highlighted that five out of six large firms were targeted by spear-phishing attacks in 2014 (Symantec 2015);
b. In 2014 more than 400 high severity zero-day[1] vulnerabilities were identified by the Zero Day Initiative[2], according to HP Cyber Risk Report 2015 (HP Cyber Risk Report 2015);
c. According to an analysis of global trends in Distributed Denial of Service (DDoS)[3] attacks, in 2014 the number, scale and complexity of DDoS attacks has increased considerably, with over 100 attacks exceeding a volume of 100 Gpb/s (100 times larger than the largest DDoS attack to hit NATO in August 2014) (HP Cyber Risk Report 2015);
d. A 2015 global survey of cyber security professionals found a 48% increase in detected incidents between 2013-2014 with respondents

[1] A zero-day vulnerability is one that is unknown by the software vendor and one for which a patch has not yet been discovered or designed. Zero-day vulnerabilities are generally regarded to be the most serious.
[2] The Zero Day Initiative is a programme that offers rewards for security researchers responsibly disclosing vulnerabilities.
[3] A Distributed Denial of Service attack floods a target system with legitimate but repeated requests with the intent to render the target offline.

reporting 42.8m incidents in 2014[1] (PWC Global State of Information Security 2015);

e. Verizon's 2015 Data Breach Investigation Report (DBIR) noted that in 60% of the cases included in their analysis from incidents across 91 different countries, attackers were able to compromise an organisation in a matter of minutes and that the average time to discover malware was months (Verizon 2015).

These figures that reflect conclusions of the industry analysis are indicative for the trends in cyber threat dynamics, with relevance not just for the private sector, but for governments and international institutions, such as NATO (Ducaru 2015). Beyond the quantitative dynamics in cyber threat evolution, recent analysis points to three major concerns that could (separately or in a concerted manner) affect the future cyber threat landscape in a potentially dramatic way:

a. The "cyber pirateering" phenomenon reflected by indications of state actors potentially turning to the criminal digital underground to commission cyber attack services and develop tools (M-Trends 2015);
b. The growing nexus between cyber and terrorism;
c. The use of cyber capabilities in relation with military of hybrid operations – the so-called cyber dimension of hybrid warfare.

While having a number of distinctive characteristics, these three major concerns are in fact quite often closely interlinked in the broader landscape of cyber threats. Therefore, while the focus on the current analysis is on the latter - the cyber dimension of hybrid warfare - the links with the first two will be also underscored.

2. THE DEFINING ELEMENTS OF HYBRID WARFARE (HW)

While there are to date many relevant articles and studies devoted to the description of HW, these studies could be considered as being just convergent building blocks towards a comprehensive and generally accepted definition. At the same time, there is so far no agreed definition of Hybrid

[1] According to 9,200 IT, cyber security and business executives polled by PriceWaterhouseCoopers (PWC) across the globe: PWC Global State of Information Security 2015.

Warfare within NATO taxonomy. However, the Allied discussion on HW has favoured a pragmatic approach towards the recent manifestations of HW, based on a comprehensive description and analysis of the phenomenon, followed by the development of a relevant strategy, instead of engaging in a scholastic, conceptual effort of adopting agreed definitions.

In essence, HW is described as a shift away from a traditional force-on-force model, to an approach which combines military and non-military tools in a deliberate and synchronized campaign to destabilize and gain political leverage over an opponent. For example, F. Hoffman highlights the difference between a context of confrontation that includes separate challengers with fundamentally different approaches (conventional, irregular, terrorist), and the HW context where competitors employ all forms of war and tactics in a coherent, sometimes simultaneous mix (Hoffman, 2009). Dedicated studies converge in describing HW as the blurring, blending and operational fusion of different capabilities and tactics into a conflict. This is accomplished by employing different types of resources, means, methods, techniques and tactics in different combinations aimed at achieving maximum desired effect (gain strategic or tactical advantage, inflict damage and loss to the adversary), at minimal cost to the perpetrator.

HW reflects the involvement, employment, pursuit and blending, at operational level, of:

a. kinetic with non-kinetic tactics;
b. regular and irregular combatants (and even non-combatants);
c. state and non-state actors;
d. physical and psychological means;
e. low-tech and high-tech means.

While aimed at generating advantage relative to the adversary at reduced cost, the HW approach aims to:

a. generate surprise;
b. seize the initiative;
c. generate deception and ambiguity;
d. avoid attribution of action; maximize deniability of responsibility for aggressive actions.

As NATO Secretary General, Jens Stoltenberg emphasized on 27 May 2015, "hybrid warfare is nothing new. It is as old as the Trojan horse. What is different is that the scale is bigger; the speed and intensity is higher; and that it takes place right at our borders. Russia has used proxy soldiers, unmarked Special Forces, intimidation and propaganda, all to lay a thick fog of

confusion; to obscure its true purpose in Ukraine; and to attempt deniability" (Stoltenberg 2015).

While the term "Hybrid Warfare" does not appear in the Russian doctrinal terminology, it is worth mentioning that one of the most compelling expositions of the essence of this concept belongs to Valery Gerasimov, the Chief of Russia's General Staff, who in February 2013 noted: "War and peace are becoming more blurred. Methods of conflict have changed, and now involve the broad use of political, economic, informational, humanitarian and other non-military measures" (in Jones 2014). All of this, he said, could be supplemented by firing up the local populace as a fifth column and by "concealed" armed forces. Mr. Gerasimov quoted the Soviet military theoretician Georgii Samoilovitch Isserson: mobilization does not occur after a war is declared, but "unnoticed, proceeds long before that" (in Jones 2014).

Russia's actions against Ukraine offer a striking example of how the coordinated overt and covert use and blending of a broad range of instruments, such as regular and irregular forces, supported by effective command, control, communications and cyber capabilities, relevant training, significant military equipment, under the cover of a carefully crafted information campaign can swiftly achieve desired goals while at the same time providing for the deniability of responsibility. This illustrates that Russia has developed and is willing to employ a hybrid approach to achieve strategic or tactical objectives.

While Hybrid Warfare is not a new phenomenon, there are, however, new dimensions or forms of manifestation that take advantage of modern technical developments and are characteristic of modern HW. Globalisation, underpinned by technological advances, particularly in the field of communications, has led to increased vulnerabilities in nations and international organizations. These vulnerabilities can be exploited in a variety of scenarios that fall short of direct military conflict. So are increasingly sophisticated cyber-attacks, far reaching complex propaganda and disinformation campaigns, as well as targeted and coordinated political and economic pressure. All of these are indicative of modern hybrid warfare scenarios, in which conventional military action may play a minor role.

Hybrid scenarios will be different in every conflict. Different elements of hybrid strategies will be combined in different ways. Individual elements will not necessarily be illegal or pose a threat in their own right, but in combination could make up for a threat to either individual Allies or the Alliance.

As with any defence or security challenge, the primary response to hybrid threats or attacks rests foremost with the targeted nation. However, the wider international community, of which NATO is an integral part, may also play an important role. No single nation, supranational entity or international organization has all the levers needed for a coherent counter to hybrid warfare. Cooperation at a multilateral level is therefore essential.

3. CONDITIONS FOR SUCCESS IN COUNTERING HW

Successfully countering hybrid strategies requires potential targets to be able:

- to recognise and attribute hybrid actions that are being directed against them;
- to have the resilience to resist hybrid actions;
- to be ready to resist;
- to have processes that allow rapid assessment and decision making;
- to be able to respond effectively.

However, apart from responding to any form of hybrid attack, the principal aim for NATO will be that its demonstrated actions to recognise, resist, be ready and make rapid decisions with regard to hybrid threats are sufficient to deter hybrid attacks, and particularly from escalation to military conflict. This requires a more dynamic approach regarding situational awareness that drives political discussion and decision-making.

Given the fact that hybrid threats would affect primarily nations, it is therefore nations that have the primary responsibility in mitigating their effects and, if necessary, responding. The wide array of possible elements included in a hybrid attack requires a 'whole of government' response that combines all national instruments. As part of their planned response, nations may turn to other Allies and to the wider international community for assistance. In preparing to counter hybrid warfare, the roles and responsibilities of nations and supporting international organisations must be clarified and practiced. It is in this context that NATO's response to hybrid warfare must be framed.

4. THE TRIAD: PREPARE – DETER – DEFEND

Framing NATO's response to hybrid threats should rely on three pillars: prepare, deter and, if required, defend. NATO will ensure that the Alliance and Allies are prepared to counter hybrid attacks, will deter hybrid attacks on the Alliance and, should it be necessary, will defend the Allies concerned in the event that hybrid scenarios escalate to military conflict. In his keynote address at the 25 March 2015 NATO Transformation Seminar, the Secretary General, Jens Stoltenberg, highlighted the fact that: "NATO must be ready to deal with every aspect of this new reality from wherever it comes. And that means we must look closely at how we prepare for; deter; and if necessary defend against hybrid warfare. To be prepared, we must be able to see and analyse correctly what is happening; to see the patterns behind events which appear isolated and random; and quickly identify who is behind and why. So therefore, we need to sharpen our early warning and improve our situation awareness. This is about intelligence, expert knowledge and analytical capacity" (Stoltenberg 2015). These are not necessarily sequential activities, but will be pursued simultaneously to ensure resilience and effective response against hybrid threats, depending on the nature of a hybrid campaign.

Prepare

Preparation to counter threats that are part of a hybrid scenario will be based – among others - on ensuring the necessary awareness to allow the recognition of a hybrid scenario.

Early warning capabilities should be boosted as a key starting point in tackling such threats. This is quite challenging, since usually previous experiences may or not may repeat in another circumstance, there is little predictability, and information flows may be expected to be inaccurate (even on purpose through the use of fraudulent media, duplicity, propaganda, etc.). NATO must be able to pinpoint early warning indicators, by identifying that hybrid threats are developing, recognizing this at the political level and reacting appropriately to ensure that hybrid campaigns do not escalate to military conflict, but are contained and mitigated at a lower level.

Building resilience is an essential element for preparing for countering a hybrid campaign. At national level, effective resilience would include coherent and up to date structures (such as crisis organization, security and defence

structures, civil preparedness, transparent and respected governance). Cyber resilience is also essential.

Education, training and exercises are also highly necessary, to create the premises for an effective action addressing hybrid strategies. Of course, preparing to counter a hybrid threat is not just about the military domain.

A network of relationships with NATO nations and non-NATO entities (countries and organizations, particularly the EU) are required to fulfil the goal of preparation. It is important that the Alliance's partners**,** particularly those adjacent to Alliance territory, are also able to resist hybrid attacks and scenarios below the threshold of military conflict. Therefore, provision of support and exchange of experience will be another strand of work. Areas that are pertinent to building resilience may include governance, institution building, civil preparedness, CBRN preparedness and critical infrastructure protection, the protection of civilians, cyber defence, energy security, etc.

Deter

The aim of this strand of work in a hybrid context is to convince the adversary that the consequences of his actions will outweigh the potential gains (including economic sanctions, political isolation, legal challenge or even military defeat). The Alliance deterrence posture, as a whole, which includes the mix of conventional, nuclear and missile defence capabilities, as well as the high level of readiness of these capabilities play an essential role in this sense.

Defend

This third strand of work is based on a hybrid adversary having been exposed and recognised. NATO will create the conditions to be able to contribute to a broader international response to a hybrid scenario. The Alliance's actions will have to be coordinated also with non-NATO entities to ensure its response measures (*on the military component*) are proportionate and synchronised. As Deputy NATO Secretary General, Alexander Vershbow (2015) highlighted "if deterrence should fail, NATO stands ready to defend any Ally against any threat. For hybrid scenarios, we may need not only to deploy conventional forces quickly, but tailored force packages with special operations forces, civil affairs expertise, and information capabilities that can work with local authorities to counter efforts to subvert or destabilize social peace. And I expect that any NATO response would then be complemented by

a much broader international effort – to bring to bear diplomatic, economic and other levers as well".

*

Just as in the case of deterrence, an appropriate narrative and effective communications strategy will be the key. The response to propaganda cannot be more propaganda. Because contrary to some who are waging propaganda campaigns against NATO, the alliance is formed of open and democratic societies. It needs to provide compelling, timely communication to counter disinformation and to base its communications efforts on facts. Its credibility is a key asset. Therefore, Strategic Communications in this respect will be the key.

Moreover, the Alliance will have to consider in the near future a series of adaptation measures, in several areas, in order to successfully counter hybrid threats. All those efforts, with a rather internal focus and including a more proactive stance, will enable:

- better abilities to anticipate and react against evolving hybrid threats;
- increased capabilities to follow the early warning indicators, through monitoring the security environment across a variety of relevant areas;
- better suited crisis response operations;
- enhanced cyber defence capabilities;
- more efficient strategic communications.

With regard to the external cooperation focused on countering hybrid threats / warfare, I would note that no single nation or organization can deal with the totality of a hybrid strategy. Therefore, effective cooperation and coordination with partners and among relevant international organizations, such as the UN, OSCE, Council of Europe, but in particular NATO and the EU, is essential in countering hybrid warfare, without prejudice to the Alliance's collective defence obligations.

A particularly important partner for NATO in facing hybrid threats is the EU. Allied Heads of State and Government at Wales (NATO Wales Summit Declaration, 2014) encouraged further mutual steps to strengthen their strategic partnership. Both organizations can provide coordinated and effective assistance to Allies and Member States in the preparation and response phases of countering hybrid warfare, while also helping their respective members identify and resolve their vulnerabilities. Among the

concrete areas where there is scope for increased cooperation with the EU are Situational Awareness, Strategic Communications, Civil-military Cooperation and Cyber Defence. Therefore, complementarities in the corresponding policies of NATO and EU and further cooperation means are sought. "We will ensure that the strategies we are developing are complementary, so that we can work together quickly and effectively in the case of a hybrid threat against any of our members". NATO Secretary General (Stoltenberg 27 May 2015) said after the meeting of NATO foreign ministers in Antalya. "The overall goal will be to ensure that, in the event of a hybrid threat, there is clarity on 'who does what and when'". The statement by NATO defence ministers (Stoltenberg June 2015), sums up the key strands of work tasked in this context: "To enhance the ability to respond quickly and effectively to any contingency, we have significantly adapted our advance planning. We have also adapted our decision making procedures to enable the rapid deployment of our troops. We have set the key elements for an effective response to hybrid threats. We will seek close coordination and coherence with the European Union's efforts in this field".

5. THE USE OF CYBERSPACE AS A TOOL FOR INFORMATION & CYBER-WARFARE

There are basically two perspectives that have to be considered when addressing the use of the cyberspace in a hybrid warfare context:

a. *Taking advantage of the opportunities of cyberspace as a domain for free, fast and effective communication* and to transform it into an efficient tool for:
    i. propaganda, manipulation and distortion of information, deception, information warfare;
    ii. recruitment and exploitation of extremists, criminals, "cyber underground" elements; hacktivists, mercenaries;
    iii. communication tool up to the level command and control instrument of choice for insurgents or terrorists (as was highlighted by the new head of the GCHQ in a FT op-ed) (Hannigan 2014).
b. The *use of cyberspace as an attack or warfare domain*, to complement and augment the effects of conventional operational engagements. This can take a number of forms such as:

i. data ex-filtration and espionage;
ii. info and data manipulation for deception effects or negative impact on institutional prestige (DDoS attacks, defacements of web-sites, identity theft or simulations for deception);
iii. cyber-attacks aimed at degrading or disrupting critical infrastructure or operational enablers / assets;
iv. cyber-attacks aimed at physical destruction of networks or critical infrastructure / operational assets.

Although for analysis purposes, it is interesting to make a distinction between these two perspectives, it is important to bear in mind that in reality they tend to converge. In fact, in Russia's military doctrine, information warfare is combined with cyber and electronic warfare, as well as with physical actions against the telecom infrastructure. This approach reflects the deliberate pursuit of impact on the physical (hardware), the logical (software) and the cognitive layers of cyberspace.

6. RECENT MANIFESTATIONS OF CYBER ATTACKS IN HYBRID CONFRONTATION CONTEXTS AND THEIR RELEVANCE FOR NATO

Cyber-attacks have been extensively observed in the context of the Ukraine conflict and associated by Ukrainian authorities and international analysts with Russian Hybrid Warfare campaign in Ukraine. Such attacks including DDoS attacks, defacements of Ukrainian websites; the hacking of data systems and malicious traffic rerouting, cyber-espionage, as well as propaganda and information manipulation were used extensively long before the Crimean crisis unfolded. Since 2010, for example, Ukrainian computer systems were targeted by a computer malware known as Snake, a powerful espionage tool that allowed access to Ukrainian government computer systems. While the links of these disruptions with Russia's Hybrid Warfare campaign in Ukraine will be further substantiated by analysis, the undisputable fact that these significant cyber-attacks have taken place simultaneously with the political and military actions related to the crisis in Crimea and Eastern Ukraine is raising significant questions and concerns. In

the same vein, the simultaneity of cyber-attacks against NATO and events in Ukraine cannot be ignored. For example, in 2014 a series of Distributed Denial of Service (DDoS) attacks targeted NATO-HQ following public statements by Allies made during the Ukraine crisis in March (assumed by "Cyber Berkut") and around the high profile Wales Summit in August and September. Furthermore, mis-information such as the deliberate mis-attribution of the CCD CoE as a host of a website aimed at targeting rebels in Eastern Ukraine (Russia Today, 26 April 2015) has been another example about how exploit cyber tools, in this case, as a supporting mechanism to demonstrate authenticity.

The recent cyber-attack attributed to the so-called 'cyber-caliphate' group, against TV5Monde (France 24, 9 April 2015) was an example of how a non-state actor, loosely affiliated with another known to be applying Hybrid Warfare techniques, has in a co-ordinated fashion deployed different types of cyber-attack in order to further its strategic objectives. This April 2015 incident involved the simultaneous defacement of webpages and social media belonging to the TV network, associated 'doxing'[1] of identity cards and other personal details of French Armed Forces personnel involved in operations against IS and the posting of a warning message aimed directly at the French leadership. More seriously, the extensively prepared attacks also rendered the broadcasts offline for two days, with the network resorting to running pre-recorded material due to the interference with the broadcasting systems. This attack was compounded further when sensitive login information for the networks social media accounts was inadvertently filmed in an interview with a journalist on the France 2 channel (BBC News, 10 April 2015).

Recent examples of cyber-attacks as part of the application of Hybrid Warfare show that state actors who misuse cyberspace also might be of significance for NATO, including cyber-criminals, loosely affiliated but co-ordinated non-state groups who disrupt cyber space and those who use it in the name of particular political, religious, ethnic or cultural ideologies (e.g. ISIL) and individuals acting under the banner of a particular ideology who wish to draw attention to specific causes through cyber-attacks; defacements or other ad-hoc actions (e.g. Anonymous). All these examples reflect the fact that NATO as an organization or Allies are already subject of the effect or the use of cyber capabilities in a hybrid operational context.

[1] 'Doxing' refers to the open publication of personal data of victims on the Internet.

7. NATO'S WAY AHEAD ON ADDRESSING CYBER IN A HYBRID WARFARE CONTEXT

In order to be able to counter hybrid strategies, the general fundamental requirements, applicable also for the cyber dimension of HW are as follows:

- increasing threat awareness, early warning, recognition and attribution capabilities;
- increasing the resilience to resist and overcome hybrid actions;
- developing capabilities and processes that allow rapid assessment and decision making;
- developing the capacity to respond effectively.

All these important aspects for framing NATO's general and comprehensive response to HW, lead to some specific requirements and priorities in framing Allied dedicated response to the relevant aspects of the cyber dimension of HW. While these cyber related aspects should be finally considered at integral part of an Allied strategy to address hybrid threats, it is worth focusing in the context of this paper of some of the cyber specific priorities.

a. Increased awareness on the dynamics of the cyber threat landscape, in general, and of manifestation of cyber-attacks in hybrid scenarios, in particular, is imperative. Regular and strategic level cyber threat assessments based on increased information sharing among allies are key in this context. The signing of the "second generation" of MOU's on information exchange and cooperation between NATO's Cyber Defence Management Board (CDMB) and national relevant cyber defence authorities, as well as the increasingly relevant analytical work NATO Cyber Threat Assessment Cell (CTAC) are of particular relevance. Blending network/signals intelligence with human intelligence in order to achieve a more refined level of attribution of cyber-attacks is also key. Furthermore, the exchange of information between NCIRC-TC and CERT-EU on the basis on a relevant technical agreement and with the private sector and academia through the NATO-Industry Cyber Partnership (NICP), as mandated by the Enhanced NATO

policy on Cyber Defence and associated Action Plan, would significantly increase awareness and early warning capacity of Allies;

b. Increased investments in the resilience of NATO's and Allies' Communication and Information Systems (CIS) remains a key priority. Through the centralized protection of NATO's CIS across more than 50 sites and the creation of the cyber defence Rapid Reaction Teams, NATO has significantly enhanced its resilience and cyber situational awareness. Follow up work is ongoing on quantitative enhancements (expanding this centralized protection to additional sites, including deployable networks) as well as qualitative hardware and software upgrades. Since the cyber resilience of the Alliance is dependent on the resilience of each of its members, the accelerated implementation of the 2013 NDPP cyber defence capability targets and the development and commitment towards the implementation of a new set of such capability targets aligned with the fast increasing threat landscape will be of great importance. A Cyber Defence Pledge at 28 reflecting Allied commitment to prioritize and expedite investments in cyber defences would be a strong political signal in this sense;
c. The employment of modern, dynamic risk analysis and management capabilities and procedures, as well as and a processes that allow rapid assessment and decision making is key in order to be effective in a rapidly evolving and quite stealthy treat environment. Analytical tools such as a Cyber Defence Decision Support System (CDDSS) as well as increasing the speed of a well informed decision making process is key in countering cyber-attacks. Constant improvement of skills and procedures through training education and exercises is closely linked with this. Various cyber-attack scenarios are be included in all NATO exercises, not just cyber dedicated exercises, such as the annual "Cyber Coalition" exercise. Relevant cyber aspects should be part of crisis management or collective defence exercises as well (including in Art 5 scenarios). These scenarios would need to account for much larger scale and persistent cyber-attacks than we have experienced – and needed to respond to – in the past;
d. NATO Crisis Management Procedures' and Manuals' (NCRSM) updates should include a particular focus on cyber defence aspects

– as well as all information operations aspects. NCRSM should also define when and how Allies national cyber defence capabilities could be employed when NATO is under cyber-attacks (e.g. similar to national kinetic defence capabilities that are put under NATO command and control when approved by NAC);

e. The study and consideration of the cyber dimension of hybrid warfare has a particular relevance in the context of NATO's operational planning, the future linking of deployable networks to NCIRC for centralized protection and the implementation of the Future Missions Network (FMN) concept;
f. It is important to link the defence against cyber-attacks to the efforts to counteract information warfare techniques, especially when these involve the use of cyberspace and when adversaries use the manifestation of cyber and info-warfare as an "operational continuum";
g. There is ample scope for increased engagement with relevant partner nations, on a case by case basis, and in the spirit if mutual interest, including through the support to help them build their own resilience. Relevant SPS projects with Jordan, Moldova, Georgia or the Cyber Defence Trust Fund for Ukraine could be considered as useful tools in this sense;
h. Based on the important principle included in NATO's Enhances Cyber Defence Policy reflecting the fact that International Law applies in cyberspace, NATO should pro-actively support, in dialogue with other international organizations such as UN, EU, OSCE, Council of Europe the establishment of rules and norms of behaviour in cyberspace as well as the development of transparency and confidence building measures in cyberspace. The cooperation with the EU, in particular, represents a key aspect in developing a comprehensive, holistic approach in countering HW in general and its cyber dimension, in particular. The signature in February this year of a Technical Arrangement on Cooperation in the Cyber Domain between NATO's Computer Incidents Response Centre (NCIRC) and Cyber Emergency Response Team of the European Union (CERT-EU), is clearly a milestone in this context.

The Enhanced NATO Policy on Cyber Defence endorsed by the heads of state and government of Allied nations at the Wales Summit in September 2014 acknowledged the increasing cyber threats against allied and NATO's

networks and provided for the development of allied defences against such threats, irrespective if they materialize in the form of "pure" cyber-attacks, or if such attack are occurring in a hybrid warfare context. From this perspective, the objectives and provisions of the Enhanced Cyber Defence Policy and associated Action Plan are fully relevant in responding to the cyber dimension of hybrid warfare. Increasing the resilience of Allied and NATO networks, enhanced cyber defence capabilities, increased awareness and early warning through information sharing, training education and exercises as well as enhanced engagement with partner countries, international organizations and industry have particular relevance for the allied cyber defences, including in a hybrid warfare context.

8. CONCLUSIONS

Due to the nexus to military operations, the manifestation of cyber in a HW scenario will provide further complexity to the dynamic landscape of cyber threats challenges and will bring forward some important and complex questions related to the utility and implications of potential operational dimension of the cyber domain (so far cyber is addressed as a domain within NATO for the purpose of cyber defence capability planning within the NDPP) or questions related to how best to strengthen and enhance Allied cyber defences in order to also deter attacks. One thing is quite evident and predictable: cyber capabilities are uniquely attractive as "weapons of choice" in any hybrid warfare scenario and it can be expected that any future hybrid campaign would make extensive use of a variety of cyber tools. Cyber-attacks could be expected to include denial of service or integrity attacks against various networks. They can impact supply chain, strategic support, political decision-making, weapons systems and may attempt to undermine the Alliance's ability to conduct operations fulfil its core tasks. Allies will have to engage into a cyber defence adaptation process with the speed of cyber, while taking full into account of the incredibly dynamics and complexity of the cyber threat landscape that will include a predictable increasing use of cyber capabilities in hybrid confrontation contexts.

REFERENCES

- "Adapting to a changed security environment": Speech by NATO Secretary General, Jens Stoltenberg at the Center for Strategic and International Studies (CSIS) in Washington D.C., 27 May 2015, http://www.hq.nato.int.
- Ducaru, Sorin Dumitru. 2015. "Amenintari in spatiul cybernetic", *Infosfera* no.4, accessed on 3 May 2016, http://www.mapn.ro/publicatii/.
- "France TV5Monde targeted in 'IS group cyberattack'" *France 24*, 9 April 2015, accessed on 15 October 2015, http://www.france24.com/en/20150409-france-tv5monde-is-group-hacking/.
- "France TV5Monde passwords seen on cyber-attack TV report", *BBC News,* 10 April 2015, accessed on 15 June 2015, http://www.bbc.com/news/world-europe-32248779.
- 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. 2009. "Hybrid Warfare and Challenges", *JFQ Joint Force Quarterly*.
- HP Security Research Cyber Risk Report 2015, accessed on 4 February 2016, http://info.hpenterprisesecurity.com/LP_460192_Cross_CyberriskFullReport_0315_gate.
- 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.
- Keynote speech by NATO Secretary General, Jens Stoltenberg at the opening of the NATO Transformation Seminar, 25 March 2015, accessed on 15 October 2015, http://www.hq.nato.int.
- M-Trends 2015: "A view from the Front Line", *Mandiant a FireEye Company*, 2014.
- NATO Wales Summit Declaration, Press Release120, 05 September 2014, accessed on 15 February 2016, http://www.hq.nato.int.
- "NATO trace 'found' behind witch-hunt website in Ukraine", *Russia Today,* 26 April 2015 accessed on 15 October 2015, http://rt.com/news/253117/-nato-ukraine-terror-site/.
- Networks reports the most volumetric DDoS attacks ever in the first half of 2014, 2014, accessed on 4 February 2016 http://www.arbornetworks.com/news-and-events/press-releases/recent-press-releases/5222-arbor-networks-reports-the-most-volumetric-ddos-attacks-ever-in-the-first-half-of-2014 .
- 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.
- Symantec Internet Security Threat Report Vol. 20 April 2015, accessed on 28 April 2015, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.
- Verisign Distributed Denial of Service Trends Report: 3rd Quarter 2014 accessed on 4 February 2016 http://www.verisigninc.com/assets/report-ddos-trends-Q32014.pdf and Arbor Networks, Press Release Arbor.