NATO TALK
around the BRANDENBURGER TOR
BERLIN

NATO'S FUTURE 2016

Deutsche Atlantische Gesellschaft e.V.

YATA! Germany

Inhalt

Introduction

In 2017, NATO will move into his new Brussels headquarters – a logistical step overdue for many but also an important signal to member states and partners that the alliance has not only withered many storms in the past seven decades but also adjusted itself to a wide range of recent shifts in its external environment and long overdue requirements for internal change.

Facing outright aggression on its Eastern Flank and after months of deliberating, planning and restructuring, NATO members have found a strategy to reassure affected allies of enduring commitment and to overcome regional divisions in Europe that could be and have been exploited in the recent past. Disagreements between members over priorities and policies have been constant companions of any international organizations and most of them stem from historical, economic or domestic factors that NATO has little influence on. And yet, the alliance has proven to be an effective platform for members to sort out dissent and come up with solutions that do not only preserve the status quo but also imply substantial steps to the future. As most political meetings in Europe this year, also the Warsaw Summit had been overshadowed by the British voters' decision to exit the European Union (EU) and the ongoing inability of the EU's member states to manage relocation, reception, and resettlement of hundreds of thousands of civil war refugees and address major migration pressures stemming from the global South in general. And yet, the summit solidified new initiatives for EU-NATO cooperation and allies underlined their unwavering commitment to peace, stability and an end to terrorist violence in its southern periphery.

But not only the policies of NATO have adjusted. Just recently, the first female Deputy Assistant Secretary General took office, and a stronger emphasis on public outreach and dialogue has already started to open up the alliance to younger faces – and voices.

The Atlantic Treaty Association founded its youth division, the Youth Atlantic Treaty Association (YATA) which has spread out to most of its 36 national associations in 1996. Ever since, YATA has served as a leading international platform for young professionals in security and defense, working alongside ATAs and fellow youth organizations to ensure that they would have a voice in the policy-making world. This year, YATA Germany is celebrating its tenth anniversary - together with more than 750 members from all kinds of international and security-related background.

With the generous support of the German Atlantic Association, the Federal Academy for Security Policy, and NATO's Public Diplomacy Division, YATA Germany holds the annual NATO's Future seminar for the third consecutive time, encouraging and deepening a transnational as well as the cross-generational debate on current security issues. It provides a platform for fruitful and enriching debates during the day and a forum for an exchange of ideas and mutual understanding, while bringing together more than 30 young professionals, scholars, senior experts, and NATO as well as government officials from 14 countries (NATO member and partner states).

When we invited the members of YATA Germany to design the seminar agenda, and their national and international fellows to comment on the questions they posed, many have stressed economic, legal, technological, and even philosophical features of security. You will find their perspectives

and policy recommendation in the collection of essays in this booklet. Same accounts for our wonderful speakers and chairs that take the time to enrich our discussions with their expertise, experience, and curiosity during the next three days.

Especially in times like these, NATO and its members have to invest in those that will shape and secure the implementation of its missions, on the one hand, and take their arguments and considerations seriously, on the other. Thank you all for participating so actively in this process and your commitment to making young voices an audible and visible part of NATO's future.

Sincerely,

Magdalena Kirchner

Spokeswoman

Youth Atlantic Treaty Association Germany

Dr. Magdalena Kirchner serves as spokeswoman of YATA Germany and associated board member of the German Atlantic Association (GAA) since May 2014. She is a political scientist and conflict researcher, currently a Transatlantic Postdoctoral Fellow in International Relations and Security (TAPIR) at the RAND Corporation in Arlington, VA and co-edits the Federal Ministry of Defense's monthly journal „Security Policy Reader". Previously, she held research positions at the German Institute for International and Security Affairs (SWP), the German Council of Foreign Relations (DGAP) and worked as Senior Project Coordinator at the GAA in Berlin. She holds an M.A. and a PhD in International Relations from the University of Heidelberg, where she also worked as a lecturer.

How to deter digital warriors? NATO and the cyberspace

The issue of security in the cyber space is of ever increasing importance – underlined by NATO's recent decision to define cyber-space as a war-fighting domain and the joint assessment that 'inter-connectedness means that we are only as strong as our weakest link.' How can the Alliance make sure that strong and resilient cyber defenses enable it to fulfill its core tasks – especially with regard to collective deterrence or even defense? Which political, strategic and technical issues need to be addressed so that NATO can really be-come 'cyber aware, cyber trained, cyber secure and cyber-enabled' in the near future? In turn, with the difference between defensive and offensive digital warfare being marginal, how can such conflicts be managed and potentially de-escalated?

Panelists

Sebastian Michael Müller is Desk Officer for International Cyber Security Affairs in the Cyber Policy Coordination Staff at the German Foreign Office in Berlin. In his role, he serves as the main advisor to the German Chair of the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. Mr. Müller is also responsible for the work on cyber security within the OSCE and the G7 as well as cyber relations with the Asia-Pacific region. Before joining the Foreign Office, Mr. Müller worked for two of the largest Public Affairs firms in Brussels and Berlin as well as for the Permanent Mission of Liechtenstein to the United Nations in New York. Mr. Müller holds degrees in International Relations and Social Sciences from the London School of Economics and the University of Zurich.

Isabel Skierka is a researcher at the Digital Society Institute at the ESMT Berlin. In her work, she focuses on industrial cybersecurity and digital policy. She is also non-resident fellow with the Global Public Policy Institute (GPPi) in Berlin and serves as a co-chair of the Internet Governance Forum Germany's steering committee. Prior to joining the ESMT, Isabel was a research associate with GPPi for two years where she helped build the institute's digital and technology program. Isabel has also worked at NATO as a Carlo Schmid Fellow, at the European Commission's DG Connect and as a visiting researcher at the Institute of Computer Science of the Free University of Berlin. In addition, she served as an editor at the German online magazine Adlas Journal for Foreign and Security Policy. Her commentary has been featured in Internationale Politik, TIME Magazine and Frankfurter Allgemeine Zeitung, among others. Isabel holds a master's

degree in international conflict studies from the War Studies Department of King's College London and a bachelor's degree in European studies from Maastricht University, including an exchange semester at Sciences Po in Paris, with scholarships from the German Academic Exchange Service (DAAD) and Maastricht University.

Dr. Olaf Theiler, born in 1963, studied History, Political Science and Philosophy in Berlin, and made his PhD at the Institute for Transatlantic Foreign and Security Policy, Political Science Faculty. In 1998 he joined the public service in the Information and Education Section, part of the Scientific Development Branch of the Academy of the German Armed Forces for Information and Communication (AIK), where he was first Senior Researcher and since 2003 Section Head for Information. In summer 2007 Olaf Theiler was send as National Voluntary Contribution to NATO-HQ where he joined the Operations Division as Deputy Executive Officer. Between October 2012 and March 2014 he served in the Ministry of Defence, Strategy and Operations Division, as Action Officer for political-military affairs in NATO and EU. Since March 2014 Olaf Theiler is Head of the Future Analysis Department in the Planning Office of the German Armed Forces, located in Berlin.

Introduction and Moderation

Mattia Nelles is a political science graduate candidate at Free University Berlin and currently he is spending a research semester in Kiev, Ukraine. His main research topics are EU & NATO, Russia and Ukraine relations. In 2012 he graduated from Zeppelin University with a Bachelor degree in Politics and Public Management. He gained work and research experience at the office of Dr. Richard von Weizsäcker, former Federal President of Germany, the e-Learning startup iversity and the Centre for Social Investment of the University of Heidelberg.

Alexander Schröder was born in 1985 in Magdeburg and serves as press officer of the Federal Office for Bundeswehr Equipment, Information Technology and In-Service Support (BAAINBw). After his compulsory military service, he pursued a career as an officer in the german armed forces and studied from 2007 to 2011 successfully Political Science at the Helmut Schmidt University / University of the Bundeswehr Hamburg (HSU). Amongst other things he became a member of the Academic Senate, member of the Faculty Council Economic and Social Sciences, a spokesperson for the Student Convention and editor in chief of the student magazine "Univok". He was the founding chairman of the university group for security policy at HSU and co-editor of the anthology

"German and European security and defense policy" (published in 2013). From November 2011 to November 2012 Alexander Schroder was Chairman of the Federal Association for Security Policy at Universities. Since May 2013 he leads the regional group Rhineland-Palatinate/Koblenz of the YATA and is member of the leadership team in the regional group of the German Atlantic Association. Since March 2016 he is Vice Chairman of the Support Association for Security Policy at Universities (FSH e.V.).

Young Leaders

Fluid Operations: NATO and Cyberdeterrence

Andrew Dywer (@cyberdwyer)

Multiple actors, lack of attribution, and hybrid action are all part of modern warfare. The growth of the internet and other digital systems has rapidly led to cyber security becoming a serious concern, from individual users to (inter)national security. This short piece examines NATO and its ability to deter actors who attempt to subvert its collective security. This follows an analysis of current difficulties in deterrence, namely difficulties with attribution, low engagement barriers, and multiple actors. These concerns are then folded into avenues for further exploration in defence and offensive operations, and what blended or hybrid responses may entail. An exploration of these issues concludes that the distinction between defensive and offensive operations in cyberspace are fluid, where 'active defence' utilising situational awareness provides the best deterrence for most actors.

Context

Alertness to cyber security sharpened with attacks against Estonia in 2007. Although never fully attributed to Russia, it exposed the potential vulnerabilities that existed among allies as dependence on assets in cyberspace has grown. Additional events in Georgia in 2008 and more recently in Ukraine have demonstrated how cyberattacks can be blended in forms of hybrid attacks that aim to destabilise states before more conventional incursions occur. NATO has responded through developing a coordinated cyber security apparatus and the formalisation of doctrine that declares that international norms of engagement apply to cyberspace.

Yet, in comparison to previous decades, there has been considerable difficulty in engaging in forms of deterrence. I identify three of the most pressing:

- Attribution: Due to the ability to mask location and to lay decoys to the origin of an attack, conventional forms of deterrence are often not applicable.
- Low Engagement Barrier: The pervasiveness of digital systems across allied and non-allied states increases the vectors and opportunities for low-skilled actors to engage.

- Multiple Actors: Due to the low engagement barrier, it is not only states that have interest in subverting NATO, but also criminals, terrorists, and hired mercenaries that may sell their services to the highest bidder.

Current policy options

We often divide defensive and offensive capacity, which enables clear doctrinal policy, but is of little use to cyber security strategy. NATO is responsible only for its own internal systems and ensuring that these integrate with allied systems. Yet, it currently has no offensive capacity of its own apart from those developed by allies.

Defensive: In all scenarios, defence of critical systems provides the best deterrence from actors in cyberspace. This includes everyday management of critical national infrastructure, ensuring good education, and the monitoring of networks along with other recognised good cyber security 'hygiene'. My PhD research on malware ecology demonstrates that maintaining good cyber security posture often prevents many subversions at entry points to the system. Yet due to interdependencies between systems, between governments and business, there will always be deficiencies in cyber security, including the opening up of previously unknown vulnerabilities such as zero-day exploits.

Offensive: Discussions of offensive capacity in NATO often focus on the trigger for Article 5, and what an armed cyberattack may constitute. This often descends into theoretical discussions over 'cyber weapons', and one which I will not go into. If we disregard the latter, the options remain either symmetric or asymmetric with conventional response. The former is often difficult due to time dependencies in developing a sophisticated response after an attack. The latter could be considered disproportionate, but is an essential arsenal for deterrence.

Recommendations

There is a false dichotomy between defence and offence in cyberspace. Ensuring security often requires scanning for threats a priori an attack or subversion. This means maintaining a high sense of situational awareness, and one that espionage traditionally provides. Therefore, developing potential offensive operations to be deployed in case of attack provide the most appropriate avenue for deterrence. Publicly disclosing an arsenal of non-specific advanced defensive preparation may deter some attacks. This addresses proportionality, enhances situational awareness and allows for preparedness. In addition, it aids with attribution as situational awareness of an array of actors can be pinpointed with greater accuracy whilst also enabling responses that do not wrongly attribute a state for non-state actors.

Policy Recommendations

1. Further enhance defensive capacity through good practices of cyber security that harmonise across allied states.
2. Develop an offensive arsenal that can be rapidly deployed in the event of an attack through 'active defence'.
3. Maintain conventional asymmetrical response.

Andrew Dwyer is a doctoral student at the University of Oxford, UK pursuing a degree in Cyber Security. His substantive research focuses on malicious software, otherwise known as malware, and their constituent ecologies. In this he considers three principal themes: movement, encounter and curation of malware. This allows an exploration of everyday spaces of malware, such as on end-point devices, through malware analysis to geopolitical discussion and discourse. The research element of his thesis involves working in malware analysis and select interviews on particularly profound pieces of malware from those who first decoded them. Prior to joining Oxford, Andrew gained a BA (Hons) Geography from Durham University, UK and worked as a market maker in products and as a management consultant in financial services at Accenture.

"New impetus and new substance" – the NATO-EU cooperation in cyber security

Pia Seyfried (@PiaSeyfried)

For the very first time, the US government formally accused Russia of hacking the Democratic Party's computer networks, and of attempting to interfere with the US election process. Cyber attacks have become more frequent, subtle and damaging. In the last decade, NATO and the EU have recognized that cyber security is a key challenge to them and to their member states. Nation-states as well as non-state actors are part of today's large cyber threat landscape.

At the Warsaw Summit in July 2016, Heads of NATO and the EU signed a Joint Declaration which lists cooperation in cyber security among its major priorities: "The time has come to give new impetus and new substance to the NATO-EU strategic partnership."1 In the light of this strategic priority the essay outlines important cooperation areas and examines further developments in NATO-EU cyber security cooperation.

In 2010, NATO's Strategic Concept identified the task of dealing with emerging security threats which led to cooperation in the area of cyber security with the EU. Since then, and confronted with shared challenges in protecting their networks, NATO and EU have strengthened their mutual support. In February 2016, a Technical Arrangement on Cyber Defense was made between the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team of the European Union (CERT-EU). The Arrangement allows both the exchange of information on specific cyber threats, and the sharing of best practices on technical procedures, configuration of networks, and partnership with industry.

Most significantly, NATO announced in Warsaw that cooperating with the EU in countering cyber threats is of strategic priority. The EU will establish a hybrid threat centre of excellence in Finland. Main cooperation areas include (under certain circumstances) even the sharing of classified information and cooperating on analysis, prevention, and early detection. NATO and the EU also pledge to cooperate regarding cyber elements in NATO's and CSDP exercises, as well as education and training, including coordinating their exercises.

The EU and NATO have made large progress in building their capacity to coordinate cyber security and defense activities among their members. Nevertheless, the authority of these two international actors remains weak.

Policy Recommendations

1. Awareness Task Force: Cyber security, being a cross-border challenge and requiring cross-border solutions, must become a central issue at highest political administrative level. NATO and EU, together with cyber experts should build a Task Force reaching out to raise awareness and technical understanding of cyber threats at national state level.
2. New focus on social media communication: The cyber threat landscape does not limit itself purely to the traditional military area anymore. The danger of disinformation – especially spread via social media – must be highlighted and actively addressed. False information can have a devastating effect, influencing a whole population's mind. A strategic communications plan is required to fight disinformation and propaganda on the internet.
3. Institutional structure: Currently, information is shared at different levels and through different institutions (see above). A clear and effective institutional structure is necessary. Europol, as one of the best functioning and recognized law enforcement agencies regarding pooling information and coordinating operational activities among EU member states, should serve as an example.
4. Public private partnership: The EU will invest up to €450 million in PPP, under its research and innovation programme Horizon 2020. With regards to defense research and industrial cooperation, the EU and NATO must foster stable cooperation with relevant private actors. The EU NIS Platform including its working groups should serve as an example in this regard.
5. Institutionalized cooperation among NATO, EU and US: Cyber security is a major policy concern to the US. All three players should work together in institutionalized forums within NATO to further develop joint cyber defense capabilities. Relevant topics for information exchange and best practice sharing should be: resilience and remediation, the development of international cyber crime law enforcement regimes, creating consistent data protection regulations.

The EU and NATO have 22 members in common. The number of shared security challenges has largely expanded. Neither NATO nor the EU alone has appropriate instruments to address the utterly complex challenge of combating cyber threats. Cyber security is the opportunity to finally bring the EU and NATO toward intensified security cooperation.

Pia Seyfried was born and raised in Berlin. After studying European Studies in France, Germany and Poland she worked as Parliamentary Assistant at the German Bundestag. Since October, she has been working as an Assistant to the Board of Women in International Security Germany. Besides, she is preparing her dissertation dealing with intelligence cooperation at the EU level. On a volunteer basis, she is a Vice President of Junge DGAP, the young network within the German Council on Foreign Relations.

Towards Effective Cyber Deterrence: Drawing the Lessons from NATO's Nuclear Experience

Maximilian Hoell (@MaximilianHoell)

Although cyber capabilities have been used as a tool of warfare alongside the conventional warfighting domains (air, space, land, and sea) only against non-NATO states (e.g. Ukraine in 2015, Georgia in 2008), examples of cyber attacks against actual NATO members abound, too. In 2007, Estonia suffered a wave of distributed denial-of-service (DDoS) attacks that incapacitated various government, bank and media websites following the relocation of a Soviet war memorial—an attack remarkably similar to the DDoS attacks that hit Georgia in conjunction with an actual military incursion a year later. Further offensive cyber actions against NATO members targeted, inter alia, the German parliament as well as the French media outlet TV5. These more prominent attacks only represent the tip of the iceberg, however. The NATO Computer Incident Response Capability (NCIRC) automatically blunts millions of cyber actions every day, with approximately 320 cyber events per month having necessitated a manual reaction in 2015.

Milestones in the evolution of NATO's cyber policy

NATO has made considerable advances in cyber since the Allies first agreed 'to strengthen … capabilities to defend against cyber attacks' in the 2002 Prague Summit Declaration, which created the NCIRC. New cyber-related bodies, such as the Cooperative Cyber Defence Centre of Excellence and the Cyber Defence Management Authority, have been set up to facilitate the Allies' coordination and development of cyber capabilities. Further milestones in the evolution of NATO's cyber policy are the Summits of 2014 and 2016. The Wales Summit affirmed that NATO's defence mandate and international law apply to the cyber domain (a cyber attack against a NATO state can thus provoke a collective response); the Warsaw Summit recognised cyber as an operational military domain—a significant step because cyber forms henceforth an integral part of operational planning, with even offensive capabilities now under consideration (although the acquisition of offensive cyber capabilities has thus far been rejected by most Allies). In NATO's Cyber Defence Pledge the Allies further pledged to 'Develop the fullest range of capabilities to defend our national infrastructures and networks'.

Why NATO's efforts to strengthen its cyber defence remain insufficient

NATO's efforts to strengthen its cyber defence capabilities represent a step in the right direction, though they remain insufficient. First, the Cyber Defence Pledge not only fails to quantify how much each Ally should invest into its cyber defence capabilities or indeed how much NATO as an alliance should invest; but it also fails to specify which systems should actually be procured or upgraded to strengthen cyber defence. Second, the cyber defence capabilities of individual member states vary greatly amongst the Allies. Whereas the United States, the United Kingdom, and Estonia have invested heavily into their cyber capabilities, other Allies have spent far fewer resources.

Because NATO's overall cyber defence is only as powerful as the weakest link in its cyber capabilities, NATO should ponder more thoroughly the question of what constitutes effective defence in the cyber domain: should each Ally develop a cyber defence capability with the limited resources available to each Ally or should cyber capabilities be developed jointly, and shared across the Alliance in an arrangement akin to NATO's nuclear sharing?

Policy Recommendations

1. When conceptualising its cyber defence posture, NATO should draw more heavily on its nuclear experience, particularly with regards to capabilities- and burden-sharing as well as deterrence. The nuclear arsenals of only three states have achieved effective deterrence for all 28 members. Only a few Allies would need to develop highly sophisticated cyber capabilities, both offensive and defensive, to replicate this success. Whereas the offensive capabilities would provide for deterrence-by-punishment, the defensive resources would achieve deterrence-by-denial. NATO's nuclear risk- and responsibility-sharing experience further suggests that a similar burden-sharing arrangement for cyber, especially with regards to the development of capabilities and the procurement of equipment, could yield very effective results. As with nuclear, some member states could provide the Alliance with the actual capabilities, with NATO coordinating the doctrine, the declaratory policy as well as the command and control systems.
2. NATO's lead committee for the governance of cyber defence, the Cyber Defence Committee, should evolve into a Cyber Planning Group to replicate the success of the Nuclear Planning Group. This would not only ensure the influence of the non-cyber Allies over the Alliance's cyber policy, but would also ensure that NATO's cyber policy evolves from the policy level into fully-fledged strategic operational planning including defensive and offensive aspects. Like nuclear deterrence, cyber deterrence will only work if NATO's own capabilities render pre-emption and punishment a sufficiently credible possibility.
3. NATO must avoid miscalculation in its efforts to enhance cyber deterrence by resolving the following issues:
    a. The problem of attribution in cyberspace, which makes deterrence-by-punishment more difficult to achieve.
    b. As with nuclear armaments, there remains a risk that NATO's efforts to achieve cyber deterrence offset a cyber capabilities arms race with countries that perceive NATO's actions in this sphere as a threat to their security. NATO must work in earnest to avoid this dynamic at all costs, for example through cyber consultations with the Russian Federation, modelled closely on the success of bilateral nuclear arms control measures.

Maximilian Hoell is a research analyst at the Atlantic Council of the UK (ACUK), and a PhD candidate at University College London. His research interests include global power shifts and hegemonic orders, as well as nuclear issues, particularly the NPT, the CTBT, NATO nuclear policy. He has represented the ACUK at strategic defence briefings at NATO HQ and SHAPE, and was

a delegate to the Nuclear Security Summit process (Nuclear Knowledge Summit 2014), and the Vienna Conference on the Humanitarian Impact of Nuclear Weapons. His professional experience further includes stints at the Comprehensive Nuclear-Test-Ban Treaty Organization, the European Commission, and the German Federal Foreign Office. He previously studied at Yale University as a UCL-Yale Collaborative PhD Student Exchange Scholar, and earned a University Diploma from the University of Montpellier, a Master's degree from the London School of Economics as well as a Bachelor's degree from the University of Oxford.

Anyone or anything could be the target: the need for distributed defence

Laurin B. Weissinger

Defending against cyber-attacks and deterring digital warriors is qualitatively different from defence in physical domains, like sea, air, and land: the realm of computers and the Internet is a massive network that encompasses billions of devices globally, and ignores national boundaries as well as the time and distance factors usually central in physical defence. Furthermore, cyber-power is scattered across states, companies, groups, and individuals but it is also highly pervasive, as military and economic interests, diplomacy, the media, and democratic procedures can be targeted by computer attacks. Cyber-risks have become part of all aspects of modern life but often remain opaque: attacks can be stealthy, particularly if the aim is intelligence gathering rather than immediate destruction. Thus, defence strategy needs to address this distribution of attack surfaces across various targets.

In an all-out war scenario, it would be prudent to use every form of weaponry available. However, using cyber only has very limited potential at this point. In consequence, this brief proposes that an all-out cyber-war is unlikely and that clandestine wars of attrition are more probable. In this scenario, aggressors would try inflicting economic, strategic, and reputational damage, as disturbance has a high potential payoff but only carries a small risk of retaliation or even confident attribution. This makes it the likely choice for state and non-state aggressors. To respond to such a diffuse and obscure threat, risk and attack surfaces have to be understood in a networked manner, including intra- and extra-organisational ties, procedures, human actors, and technology. In cyber, risks and the potential of mitigating risk often flow in both directions: a security appliance prevents some attacks but may itself become a target, as recently announced bugs in unsupported but widely-used CISCO firewalls demonstrate. Higher level risks also matter and are difficult to defend against; for example, the successful exfiltration of data from the US Office of Personnel Management has uncovered CIA operatives, exactly because their details were not part of the leaked data.

Defence mechanisms must be distributed to fit this complex and multi-dimensional risk environment. Theoretically, the cyber-attacker is always in an advantaged position – she has to find only one point of entry while the defender tries to defend them all. However, even though disturbance strategies are usually asymmetric, attacker economics remain relevant: the better

secured a system, the harder it is for attacks to succeed. Thus, the frequency and effects of successful attacks or continued disruption strategies can be reduced considerably by increasing the water-level. Attackers – and not only defenders – have a budget of time and resources that they must allocate and cannot exceed.

To create an attacker-unfriendly cyberspace, distributed defence must be pursued, for which five starting points are outlined in this brief's policy recommendations.

Policy Recommendations

1. Security and risk analyses at NATO and elsewhere must consider the many ways in which organisations are vulnerable, including insider attacks, and security efforts have to be designed accordingly.
2. NATO must advocate improved out-of-the-box security, so that devices, including IoT type products, ship with security features enabled and tested for weaknesses. This is because many individuals and firms linked to NATO member states do not have the know-how to secure themselves.
3. NATO should support research into cybersecurity, and promote security research and investments in the member states: financing independent research in cybersecurity is vital for states and organisations that heavily rely on information technologies.
4. Attackers will target whatever organisation shows weaknesses or seems opportune strategically. Thus, NATO must promote the creation of public-public, public-private, and private-private partnerships that facilitate information and knowledge exchange.
5. Defence enforcement is probably the most important issue in defending cyberspace: audits are often a farce, regulation regimes often fail to address security properly, and, as a recent paper by RAND underlines, many companies choose lax security measures because repercussions for data breaches are minimal. Yet, risks in cyberspace travel easily between different entities and organisations, and thus NATO members must push for regulation that forces companies and state institutions to invest in security and adopt more stringent security measures.

In conclusion, cyberspace is a security challenge because it is borderless and complex. Defence must be distributed and designed to deal with the particularities of the cyber-realm. As all-out cyber-war is unlikely, and so NATO must focus efforts on strengthening the security posture of not only states but also companies and citizens, for which this brief has made five recommendations.

Laurin B. Weissinger is currently a doctoral candidate and researcher with the University of Oxford, where he is associated with Nuffield College, the Exlegi Institute, Department of Sociology, and the Cybersecurity Centre. His academic background is mostly in the social sciences, while his professional experience is in information technology. Broadly, his research is about IT-Security with a strong focus on multidimensional security. Currently, he is focussing on the following topics: cooperation among security professionals and different organisations, human-computer networks and dependencies, standards and regulation, risk analysis and mitigation, and lastly the resulting security strategies. He uses a variety of methods, including qualitative, quantitative, and network analysis approaches to address these topics and associated questions.

Achieving Cyber-Deterrence

Jurgen Rudi

The complexity of Internet will continue to grow. According to CISCO, by 2020 there will be 50 billion connected devices on the Internet and around 4 Billion active users. From the very first malware in 1986 to today's advanced malware such as Stuxnet, Snake or Regin, the evolution of cyber threats in this interconnected world is undeniable. While the internet is evolving so are cyber-criminals. Modules such as zero-day vulnerabilities, malwares and botnets are being offered on the commercial market by cybercrime actors with the intention to advance hacking activities as much as possible.

In the cyber reality the "Hegemonic Stability theory" in which stability is maintained by an actor which is more powerful than all others does not apply. Cyber criminals today conduct any kind of cyber activities, mainly based on financial agreements, to the extent that it is difficult to affiliate malicious activities to a specific state or group. Threat actors targeting NATO networks are often part of complex organizations, organized in teams that combine different roles, expertise and experiences. Their activities are oftentimes coordinated and act upon specific objectives. Thus, the malware is sophisticated, the command and control (C&C) infrastructure is obscure and the modus operandi incorporates enough tricks to make analysis as difficult as possible.

Deterring malicious cyber activities is seen as an ambiguous goal among cyber community and this is mainly because of:

a. Keeping aggressors at risk is viewed as impossible from a technical perspective.
b. The use of force is prohibited under the UN Charter's Article 2 (4).

Thus, the predominant idea is that since it is assumed impossible to deter, all the focus should be put on developing defense capabilities to be able to turn down potential malicious cyber activities. Making cyber-attacks more expensive and building trust and capability within the cyber defense community are among the different approaches proposed for achieving cyber defense.

Be that as it may, there still exist ways to build cyber deterrence strategies that can produce result on the real world, especially when referred to state-actors. Furthermore, cyberspace can be used as another diplomatic tool to achieve military deterrence. In general terms, cyber-deterrence can be viewed as as the ability to hold the adversary critical cyberspace strategic objectives at risk. As detailed in "Conflict and Deterrence under Strategic Risk", 2010 paper from Sylvain Chassang and Gerard Miquel "holding strategic objectives at risk" means to intimidate the critical cyber infrastructure of the adversaries. One way to achieve this is by publicly communicating NATO's retaliatory and/or autonomous cyberspace strategy and capability, to a degree that will not disclose details to the potential bad actors regarding specific tools or techniques to achieve the end result.

In both strategies technical and human components are involved. Technical component aims to analyze the malicious attack (the code, packets, and functions) in an attempt to trace back to hackers. Human component's goal is to analyze the technical outcomes in order to associate the attack with an organization or individual. Once the association has been identified, NATO should

not attribute blame to the individual/organization but to the state itself which should be held responsible for any cyber aggression ranging from the IP space of its geographical borders. In this context it is to highlight that the cyber threat perception highly differs across political and cultural systems across nations. So far there is no single institutional construction that can act as a representative model for others. Even though in principle nations agree with that governments should be held responsible for cyber activities (defensive/offensive) the exact role and responsibility that the military or other ministries/governmental institutions should play is not clear and this is mainly due to the fact that still cyber crises involving critical infrastructure as of yet only occurred sporadically.

Policy Recommendations:

1. NATO and Allied Nations should cooperate in the development of a common methodology for threat assessment by analyzing the actors and their potential impact. NATO cyber Defense security devices and processes should be upgraded based on the feedback provided by the common assessment.
2. Cyber threat information sharing with private sector, as well as creation of a trusted network of experts on cyber defense and research funding for cybersecurity.
3. Publicly communicate cyber capability to a degree that will not disclose technical details to potential adversaries, as an attempt to intimidate bad actors.
4. Attribute blame to states which should be held responsible for any cyber aggression ranging from the IP space of their geographical borders rather than to an individual/organization.

Jurgen Rudi is a Computer Scientist (MSc), specializing in Information Security & Management and Communication Systems. He is a professional with 3 years of experience in the field, including the positions of Information Security Manager at the Intelligence Military Agency of Albania, Research assistant on Cyber Defence at the of Security and Trust (SnT) Research Centre in Luxembourg as well as Information and Knowledge Manager at NATO Land Command (LANDCOM) in Turkey. Currently, he is working as an intern at J5, Strategic Planning Division at the Supreme Headquarters Allied Powers Europe (SHAPE) in Belgium assigned as Information Manager.

NATO's Future: Securing Cyberspace

Donna Artusy (@d_arts)

The North Atlantic Treaty Organization (NATO) holds a critical strategic position in the international community with regard to increased cybersecurity and responses to future cyber attacks. Given NATO's recent recognition of "cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea," (NATO 2016a) it is clear that cyber attacks are of strategic concern to the international community. As NATO Secretary General Jens Stoltenberg stated, "...a cyber attack can trigger Article V, meaning that a cyber attack can trigger collective defense." (NATO 2016b) Given this important step, NATO must set additional precedent in order to establish consistent responses to cyber attacks and strengthen enforcement provisions.

The impact of cyber attacks increase annually with a projected cost of $2.1 trillion worldwide by 2019. Attribution in cyberspace is difficult and the scale of attacks is varied, ranging from Distributed Denial of Services (DDoS) to more sophisticated Advanced Persistent Threat (APT attacks) as well as cyber espionage. It is concerning that even when attribution has been established and the aggressors made known, the responsible parties are met with insignificant consequences and minimal punishment. This is due largely to the lack of a universal legal infrastructure and an enforceable plan of action. This was evident when Russia attacked the Ukrainian power grid in 2015, and faced minimal consequence for its actions. Creating a deterrent effect for future attacks is important to curbing cyber crime, but the current lack of recourse against aggressor states is detrimental to that effort.

Currently, there are several bilateral agreements in place that are excellent steps towards international cooperation, but none provides clear repercussions against aggressors or enforcement mechanisms. These include agreements between the United States and United Kingdom, the US and Israel, as well as international agreements such as the African Union Convention on Cyberspace Security and Protection of Personal Data, the International Multilateral Partnership Against Cyber Threats (IMPACT), and the Cybercrime Convention. NATO is in an ideal position to create the first doctrine on cybersecurity that defines if and what type of force can be used against an attacker (conventional or otherwise), how NATO members will apply collective action in cyberspace, and at what threshold Article V will be triggered.

<u>Policy Recommendations</u>

To strengthen international cyber norms under the auspices of NATO moving

1. Implementation & Reinforcement: Ensuring implementation of the Computer Emergency Response Team for EU institutions (CERT-EU) to promote information sharing amongst EU and NATO member states is paramount. The current framework encourages information sharing, but this is often met with bureaucratic inefficiencies and logistical problems. With valuable information acquired by allies, this information must be shared (where permitted) to minimize the risk of detrimental cyber attacks.

2. Temporary Legal Body: It is essential to engage with international courts to create a temporary legal body that will focus solely on cybersecurity concerns. This legal entity will oversee the creation of a doctrine that is comprehensive, acceptable, and observable by all NATO members. This will be an intermediate step towards the establishment of a permanent legal institution.
3. Executive Oversight Team: The team will provide executive oversight to implement the new doctrine set forward by the temporary legal body. Creating an oversight team will ensure uniform application of predetermined norms. This is necessary because the implementation of a new set of norms in cyberspace will be extremely daunting, and an oversight team can ensure that responses are appropriate. The team will ideally be composed of representatives from NATO member states, encouraging fair representation.
4. Permanent Legal Body: After the aforementioned steps have been put in place, it will be necessary to establish a permanent legal institution or division of an international court that is dedicated to cybersecurity. It is difficult to propose where this permanent court would be housed due to jurisdictional issues, but the International Criminal Court may be the most relevant legal body that has the capacity to address legalities relevant to cybercrime. The legalities of cyberspace are somewhat ambiguous and undefined; therefore it is necessary to ensure that there is a reliable legal body that can set precedent in the field.
5. Means of Retribution: Establishing means of retribution for violations of the newly created doctrine. This may include measures such as kinetic responses or diplomatic actions (negotiation, use of sanctions).

Literature

NATO (2016a): Warsaw Summit Communiqué, North Atlantic Treaty Organizationhttps://ccdcoe.org/sites/default/files/documents/NATO-160709-WarsawSummitCommunique.pdf, Paragraph 70.

NATO (2016b): NATO Press Conference, Secretary General Jens Stoltenberg, June 14, 2016, http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en.

Donna Artusy is currently a graduate student at Georgetown University in the School of Foreign Service, Security Studies program. She is focusing on technology and national security issues, with a specific interest in cyber security and nuclear non-proliferation. She double majored in history and political science at the University of California, Berkeley. Previously, she completed the International Security and Intelligence program at the University of Cambridge, and has held internships at the Center for Strategic International Studies (CSIS) and the United States Department of Justice in Washington, D.C., and worked at a private international law firm.

NATO & Europe Need a Perspective of Cyber Deterrence

Alexander Schröder

The Cold War was a balance of terror. The Soviet Union and the United States of America kept the other block at a distance with their nuclear weapons. Armed to the teeth, both in the West and East one was afraid of the first strike of the other side. But this balance of terror also brought about stability. An intervention in the other block's sphere of influence had become unthinkable, as it would have meant a war with no winner - whoever shoots first, dies second. Ultimately, the enormously expensive armament race brought down the Soviet Union.

Once again the world has changed. Instead of two great power blocks, there are a large number of political and geostrategic actors in the world. Boundaries are blurred, most countries and their economies are interwoven with each other through common economic spaces, interstate institutions or world-wide communication relations. National borders play hardly any role in people's daily activities. In the Internet of things machines will also communicate with each other. It is certain that steady communication reduces the risk of escalating conflicts.But this thesis is only proven for democratic state structures. The downside of technological advances is that progressive technology is also becoming easier and cheaper to interrupt.

This also means that it is becoming more and more expensive to maintain the protection and functioning of network infrastructure. At the same time, it will be easier and cheaper to attack these network infrastructures from cyberspace. The example of so-called sricpt kiddies is familiar to everyone today. But nowadays even botnets are available for little money. Highly specialized viruses and worms can be purchased for a few millions, tailored to the intended attack target. In a world traversed by IT-networks terrorist groups or even criminals are basically capable of doing this. Only the right attack target must be selected. Without electricity, for example, networks do not work, without networks, the globalized world stands still. Governmental security tasks in cyberspace must be integrated into measures of internal and external security. At this point, it is also fundamental to differentiate between cybercrime, cyberterrorism and cyberwar. Because legalism always means keeping the right measure, cyber attacks must be correctly identified and answered with adequate countermeasures. The boundaries between external and internal security become increasingly blurred.

But also in a cross-linked world, the basic task of every state is to protect its citizens from security threats and to perform the monopoly of violence within its borders. Can a government ensure this protection in cyberspace? It can, for example, by protecting the IT-network infrastructure. But it is certain that in the many million lines of code in software there will be security gaps which can be exploited. So it is better when from the beginning on a potential opponent assumes an attack to be hopeless. In the logic of the cold war this means that the enemy must calculate on his destruction in case of starting an attack. By knowing that there is no possibility of winning, the attack is not started at all. Therefore, countermeasures to attacks in cyberspace must always include an adequate response. These countermeasures must be scalable, so as not to paralyze the networks of an entire country, for example, while handling a simple data theft[VU1] . Identifying und

attributing an attack is difficult by many possibilities to conceal or falsify the own location within the net. But only if an opponent is clearly identifiable he can be effectively combated. This is relevant for cyberwarfare as well as the fight against cybercrime. Deterrence in cyberspace means keeping the opponent from attacking due to fearing the certainty of an adequate answer - online and offline. The interaction between measures in cyberspace and police or ultimately military actions acts as a deterrent. These abilities and possibilities of interactions are strengths of state structures.

NATO and the EU are challenged to act collectively as agenda setter and set standards. The following five objectives must be particularly intensified.

Policy Recommendations

1. strengthen the research and development of IT forensics in order to be able to attribute attacks quickly and unambiguously,
2. implement globally valid criteria of attribution,
3. cyber capabilities and tools have to be used purposefully,
4. cyber capabilities must be scalable and proportionally escalatory,
5. establish and enforce international law for cyberspace.

Deterrence in cyberspace is not about massive retaliation or flexible response such as in the Cold War. It is about scalability the countermeasures for threats in cyberspace within the existing framework of internal and external security.

Cyberspace as a Battlefield of Information Warfare

Mariita Mattiisen (@mattiisen)

Cyber in the 21th century is a part of our daily routine. Everyday activities have in many cases moved to the cyber space. Although these developments are making our lives easier and faster, they also possess new kinds of threats we need to deal with. Systems must be secured and protected from hacking or cyber attacks, being trustworthy for their users.

NATO as a defensive organization is also defensive against cyber and hybrid threats. First steps against these threats have already been taken, but threats are becoming both blurrier and more complex.

On the one hand, NATO has recognized Russia as a threat to NATO, which must be dealt with. In addition to real military threat from the East, however, our societies are vulnerable through the cyber space dimension. The Russian military and security services have systematically prepared themselves for war in cyberspace. In 2007, when cyber attacks against Estonia occured, which led NATO to establish the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in the country. At the Wales Summit, NATO agreed that cyber attacks can threaten transatlantic

stability and security, and recognized that cyber defence is part of NATO's core task of collective defence. This year's NATO Summit officially recognized cyberspace as a military operational domain, which must be introduced into NATO's defence planning processes. Strengthening and enhancing the cyber defence of national networks and infrastructures was declared as a matter of priority.

Even though technical aspects are extremely important, the cyber space must be seen as a bigger picture, which is used also for propaganda, spreading disinformation, manipulating citizens.

"Information warfare's main tasks are to destroy the key military, industrial, administrative sites and systems of an enemy, to inflict psychological and information damage on the military and political leadership as well as the troops and population" (Joyal 2016). These operations in the cyber space are much harder to detect and therefore to deter. This kind of information warfare involves confusing, distracting, dividing and demoralizing. It is not a call to independent critical thinking but an attack on the whole idea of truth (Lucas 2016). Information warfare itself is not particularly new, however, due to the development of technology and cyberspace, it has reached to a new dimension, being therefore a significant challenge to the West. It has been understood, that we are facing really diverse threats today which are much more complex than the ones known so far, and as a result, in 2014 NATO StratCom COE was established in Latvia.

As warfare and threats are becoming more hybrid, hybrid countering measures must be taken into account.

Policy Recommendations

1. Cyberspace used as a battlefield for information warfare is a real threat to our societies. In the free media space, especially in social media, it is much more complicated to protect citizens against harmful messages, disinformation, falsified facts or propaganda. Against these technical and informational threats we face in the cyberspace, deterrence against hybrid threats directed by the NATO HQ should be considered in addition to military deterrence. For now, hybrid threats are mainly dealt by member states or COEs. Clear measures by HQ can increase the effectiveness of deterrence.
2. More attention should be paid to the cyber deterrence, including deterring propaganda and disinformation, which are widely used by Russia (but also by ISIS) via internet and social media. Involving member states private companies and NGOs for more effective countering should be considered. Private companies and member states' NGOs have better overview of their own countries and also capabilities to support HQ to counter these kinds of threats. For example, private TV channels or newspapers can help to spread right information, NGOs can organize public events for member states citizens etc.
3. One of the key elements in successfully deterring an information warfare are our own informed citizens, who are educated and can think critically, can separate falsified facts from the real ones and can identify the difference between news and propaganda. Thus, systematically given adequate and fact based information to our societies can help to achieve it, combined with different workshops and seminars to targeted groups. United, informed and smart people is the best tool to fight against these digital warriors we face today. Information

should be provided by the member states' and NATO Associations in every country in accordance with the HQ.

Literature

Paul M. Joyal . "Cyber Threats and Russian Information Warfare", Winter 2016
https://www.jewishpolicycenter.org/2015/12/31/russia-information-warfare/

Edward Lucas. "Russia's information warfare", 11.06.2014.
http://www.politico.eu/article/russias-information-warfare/

Mariita Mattiisen is a project manager at the Estonian Atlantic Treaty Association (EATA). Holding a master's degree in international relations from the University of Tartu, her main research areas are the Eastern Europe and Russia, information warfare, security and defence, on which she has also published articles. After graduation, she worked as an analyst in the law and research department of the Estonian Parliament. Before starting at EATA, she was a director of the European Movement Estonia. She has participating in different conferences and workshops both as a listener and as a speaker in the Western countries but also in Russia and Belarus.

In for the long run? NATO's future role in crisis management

Preventing and managing crises, stabilizing post-conflict situations and supporting reconstruction – how attainable are these goals for NATO and how can existing strategies and instruments be improved? Crisis management operations have played a crucial part in NATO's post-Cold War transformation. But to what extent can peace-keeping missions like KFOR in the Balkans and RSM in Afghanistan be expected to also be a part of NATO's adjustment to the current "Article 5-World"? If so, what are the lessons that can be drawn from past operations and to what extent can they be rendered useful for future missions in a context of "intervention fatigue" on the one hand and an unraveling security environment on the other?

Panelists

Lieutenant General Frank Leidenberger assumed his position as Commander DEU Elements MN Corps/Basic Military Organization at the German Army Headquarters in Strausberg in September 2016. Previous to this most recent deployment to Afghanistan as Chief of Staff, Headquarters Resolute Support June 2015, he was the Director of the Planning Office of the Bundeswehr. Prior to that posting, he served as the Deputy Chief of Staff for Operations of the Bundeswehr Response Forces Operations Command from November 2010 to May 2012. From July 2008 to November 2010 he commanded the 31st Airborne Brigade in (OLDENBURG). During that time also deployed to Afghanistan to serve as the Commander of ISAF Regional Command North from December 2009 to June 2010. He served in the Armed Forces Staff in Berlin in the Military Policy Division (2001) and in Bonn as Branch Chief "Transformation and Concepts" in 2006 as well as Chief of Staff, Special Operations Division in 2005. He was Chief J3 EUROCORPS from October 2002 to February 2005. During this time he served in Afghanistan as the Deputy Chief of Staff, HQ ISAF from July 2004 to February 2005.

Mihai Carp is currently Deputy Head of Section in the Operations Division of the NATO International Staff in Brussels. In 2011, Mihai Carp was the principal contact point in the Operations Division for NATO's operation in Libya, Operation Unified Protector. Over the last few years, he has dealt primarily with maritime and counter-piracy issues, as well as NATO relations with the African Union. Since 2003, Mr. Carp has been dealing primarily with NATO's "new" missions, notably Afghanistan. As the principal desk officer, he travelled frequently to Kabul and liaised closely with the Office of the NATO Senior Civilian Representative. He has dealt extensively with NATO operations in the Balkans and was a member of the NATO Crisis Management Teams in South Serbia and Macedonia in 2000 and 2001. He also served as Political Advisor to Commander KFOR in 2000. Mr. Carp has been focusing primarily on Crisis Management Operations and political-military matters since 1999, after having joined NATO in late 1997 as a speechwriter for the Secretary General.

Nicole Birtsch is a research associate in the Asia Division of the German Institute for International and Security Affairs in Berlin since 2016. Prior to that, she worked as a policy advisor to the Joint Secretariat High Peace Council in Afghanistan and served as Head of the Department for Peace and Conflict Studies at the National Centre for Policy Research (NCPR) at Kabul University from 2008 to 2011. In that position she supervised all aspects of the Pathways process in Afghanistan. Ms Birtsch's intensive practical experience has given her a deep knowledge of the socio-political situation in Afghanistan, as well as of the initiatives, actors and stakeholders involved in the peace process. Prior to coming to Afghanistan, she worked with the German organization FriEnt (Working Group on Peace and Development), engaging with victims and perpetrators in transitional justice and peace building processes.

Introduction and Moderation

Dr. **Magdalena Kirchner** is a Transatlantic Postdoctoral Fellow in International Relations and Security (TAPIR) at the RAND Corporation. Previously, she held research positions at the German Institute for International and Security Affairs (SWP) and the German Council of Foreign Relations (DGAP) in Berlin. Since 2009, Dr. Kirchner works as editorial journalist for the Security Policy Reader, jointly published by the Federal Ministry of Defense and the German Armed Forces. Throughout 2014 and 2015, she worked as Senior Project Coordinator at the German Atlantic Association and had been a member of the extended board of Women In International Security Germany. Before relocating to Berlin in 2012, she had been a

lecturer at the Institute for Political Science at the University of Heidelberg, head of the Working Group "Conflicts in the Middle East and Maghreb" of the Heidelberg Institute for International Conflict Research, and gained international work experience in Turkey, Israel and Jordan. Since 2014, she serves as spokeswoman of the Youth Atlantic Treaty Association Germany.

Christian Zrenner is currently pursuing his bachelor degree in Governance and Public Policy at the University of Passau in his final year. In his internship at the German Permanent Mission to the United Nations in Geneva in 2015, he gained considerable insight in the work of the United Nations Human Rights Council and the Geneva Conference on Disarmament. Not only during this time he has developed a passion for foreign and security policy. He is pursuing this passion in his position as vice-chairman of the local group of the Academic Association on Security Studies at the University of Passau as well as in his position as an active member of YATA Germany by organizing high-level events and engaging in grass-root work in order to raise public awareness for the security challenges of our times.

Young Leaders

NATO's future role in crisis management needs the European Union

Ionela Ciolan (@IonelaCiolan)

The annexation of Crimea and the conflict in Donbas are the ignition of the refocus of NATO's main objective from crisis management to collective defence. After 25 years of crisis management operations in Afghanistan and Western Balkans, the Wales Summit was a sign of a return to "back to basics". Nevertheless, the Warsaw Summit declaration still emphasizes the alliance's commitment to the second "C": crisis management. As the Euro-Atlantic security is threatened by a multitude of crisis and conflicts (from Libya, Syria, Iraq, the dangers posed by the so-called Islamic State, a volatile security environment in Afghanistan, the refugee crisis and a revisionist Russia), it is clear that NATO has to engage in a long-term transformation and adaptation in order to properly respond to 21st century security threats.

As the financial crisis and austerity measures took a stance in member states' defence budget for the past years and the increasement of it is marginal, the long-term approach to crisis response operations will be limited. The Warsaw Summit showed there is a divided agenda within the allies and the shared-burden principle is still ignored, as the United States is contributing to more than 70% of NATO's defence expenditures.

Moreover, due to complex and multi-level conditions of the security threats – terrorism, fundamentalism, failed states – and a greater involvement of non-state actors, a suitable reaction is not always covered by a military response. A civilian and political answer can foster a faster and better solution in certain cases. As NATO's hard power and its military response are deemed insufficient to tackle these challenges, the strategic partnership with the European Union signed during the Warsaw Summit is a suitable response. This cooperation will cover the gaps in maneuver for the Alliance by providing it with complementary crisis management instruments of action and reaction. A better cooperation in defence planning between the two organizations can led to an improved dialogue, convergence and to avoid duplication of resources.

During the Summit, NATO and the EU have agreed on several objectives: the development of playbooks on hybrid threats and a mechanism to fight against them. Moreover, the cooperation will be expanded to include cyber security missions, exercises, education and training; interoperable, complementary defence capabilities; increase of collaboration in areas of defence industry and research within the Euro-Atlantic region; organization of parallel and coordinated exercises starting in 2017; increase the resilience of and strengthen the defence and security capabilities of partner countries through various joint projects.

NATO-EU crisis management cooperation can be built on the existing instruments and operations. The alliance intervention in Afghanistan and in Libya showed the effects that state failure have on the regional and global security and the limits of the post-intervention military response. Since the European Union has conducted 28 military and civilian missions around the globe, its expertise on the civilian part of crisis management (from fostering the rule of law to border, police, justice reforms) can help in constructing a joined and comprehensive approach to crisis management actions.

NATO's collaboration with the European Union on patrolling the Aegean Sea and tackling the illegal trafficking was of real importance in reducing sea arrivals to Greece. It was also a great exercise of information sharing and logistical help between the alliance, FRONTEX, Turkish and Greek coast guards and a lesson learned for the new established maritime operation Sea Guardian.

Since today's warfare combine conventional tactics with unconventional elements, only a European Union-NATO plan based on interoperable, comprehensive and complementary collaboration will be capable of managing this millennium' security challenges. While this is a promising start to foster consultation and interoperability between NATO and the European Union, putting into practice the political goals will need to keep in mind some of the following

Policy Recommendations

1. NATO and EU will have to deal with the burden sharing through a combination of institutional capabilities and by incorporating NATO's military assets with the EU's civilian expertise with a distinctive distribution of tasks and responsibilities.
2. Measures to increase the resilience of member states and partner countries to security threats should include early warning mechanisms, education, joint exercises and training.
3. Fighting threats stemming from non-state actors through preemptive diplomacy and the EU's soft power capacity (supporting good governance, adopting projects on counterterrorism, and creating country-specific capacity-building programs).

4. Creating a joint Immediate Response Council to urgent crisis management actions.

Ionela Maria Ciolan is a third year PhD candidate in International Relations at the National University of Political Studies and Public Administration (NUPSPA), in Romania. She is currently researching on the European Neighborhood Policy in Eastern Europe and EU-Russia relations. Her academic work includes two ongoing research projects and a teaching assistant position on a course about NATO. Apart from that, Ionela is also a human rights activist and educator. She is the founder and president of the only human rights activists group of Amnesty International in Romania (Amnesty International Bucharest Group). In addition, Ionela is an expert on European Affairs to Strategikon, a Romanian based think tank. Her professional work includes a research mobility at the Centre for EU-Russia Studies (University of Tartu), a Professional Fellowship granted by the U.S. Department of State, an internship at the Chicago Coalition for the Homeless, a traineeship at the European Parliament.

The Future is Coming: A Context for NATO's Crisis Management

Lianne de Vries

NATO's concept of crisis management has adapted to the security challenges on its Eastern and Southern periphery. However, simultaneously, the future security environment is taking shape. It is characterized by a rapid rate of change and complexity as the grand strategic trends (demographic, environmental, technological, political) intersect and influence each other in multiple ways. Surroundings will become more interlinked and multi-disciplinary, supported by disruptive technology and occurrences and requiring a constant reinvention of oneself and one's position. This requires an equally dynamic, ready and tailored approach. Following are recommendations to support this posture.

The North Atlantic Council (NAC), comprised of representatives from each member state, gives the political 'green light' via consensus to NATO operations. Committees and organs responsible for organizing the dimensions of a crisis management operation support them. Tasked with consolidating the national positions, interests and efforts of 28 member states, reaching the vote is a lengthy process that forms a weakness in NATO's ability to take action swiftly. This could impede swift response during crises when decisive action is needed, and therefore forms a weakness. NATO should establish an emergency council that, without bypassing the authority of the NAC, will decide initial and limited deployment for the most time-sensitive situations. The emergency council would consist of the NATO Secretary General, the SACEUR, and a third or fourth party depending on the situation. The NAC would retain the power of review, recall, and decide the duration of the operation.

In the complex security environment, NATO should intensify its network-based approach to crises. In addition to the contributions of its member states this provides a dimension of inter-agency partnerships with the private sector, civil agencies, NGO's and philanthropists (both NATO and non-NATO) in the phases of crisis prevention and reconstruction. The prevention of crises would be strengthened by an inter-agency monitoring system with strategic international and regional partners. Such strategic partnerships would also enhance NATO reconstruction efforts by, for example, facilitating a consultancy firm to offer advice on business and agricultural re-development or to have a philanthropist invest in solar energy batteries to reduce electricity dependency. Via innovative collaboration NATO's mission is more likely to succeed, and through the partnerships NATO's message will have a wider reach and its image and public relations will also be enhanced.

VJTF simulations have exposed weaknesses in the harmonization between nations while moving troops and supplies. This can also affect NATO's crisis management and ability to quickly amass troops and supplies and move them across states to a crisis area (both within and peripheral to NATO territory), as each nation has individual legal procedures in place that influence this process. To strengthen NATO's timely response, it should facilitate further negotiations on legal issues to enable easier and faster movement of troops and supplies.

In addition to the Alliance's peripheral focus, it should also strategically shift from external crisis management to internal. Instability and threats are permeating into NATO's territory as geographical borders decline in their security significance. This provides new, relevant opportunities for NATO while it can also increase its visibility among the population. NATO should adapt its planning and presence accordingly.

Nations are adjusting their security structures, capabilities and international cooperation to the changing security threat. This particularly includes terrorism from individuals already inside NATO territory, cyber security, infrastructure and intelligence. To increase efficiency and effectiveness, it is advisable for the adjustments to be fine-tuned among NATO Allies. Due to its experience, NATO is the best-placed organization to have a coordinating and facilitating role to streamline efforts between nations. Feasible domains include intelligence by standardizing procedures and software for easier electronic intelligence sharing; determining any security threats posed by mass migration and synchronizing national defensive efforts; and structuring a single cyber security strategy that permeates national levels and their approach to cyber issues. This will further facilitate interoperability, signal unity to potential adversaries and improve NATO's position to act in crises.

<u>Policy Recommendations</u>

1. NATO should establish an emergency council to increase the pace of decision-making
2. NATO should strengthen its network-based approach
3. NATO should further legal cooperation and adaptation within the alliance
4. NATO should adopt a coordinating role between national security efforts

Lianne de Vries has completed her MA in Strategy and International Security and holds a Bachelor's in International Human Resource Management. She is particularly interested in the future security environment, grand strategic trends, strategic positioning, the Transatlantic Alliance

and multidisciplinary and cross-cultural approaches to issues. In the increasingly dynamic and challenging security environment, NATO has the unique potential through its shared values, culture and beliefs. Through innovation and adaption, the Alliance can position itself to successfully meet the future security environment and ensure transatlantic security. Lianne is vice-president for YATA Netherlands and participates in the Dutch Ministry of Foreign Affairs' youth think tank 'The West Wing'. She is part of the Atlantic Council's 'Future NATO Fellowship', enjoys writing articles and is currently preparing for her internship at NATO ACT in 2017.

A future role of NATO in stabilizing Ukraine

Miroslava Grausova

The past two decades have witnessed significant transatlantic engagement with crisis management. The wars in the Balkans challenged the transatlantic community not only to intervene militarily but also to engage in post-conflict reconstruction and long-term institution building efforts. Crisis management is being currently performed in Ukraine, where NATO has been reinforcing its support for capability development and capacity building in order to contain internal strife and provide the country with a stable security platform.

Recent NATO-Ukraine Relations

At the Bucharest summit in April 2008, NATO launched its open door policy under which Ukrainian membership became formally possible. However, two years later, President Viktor Yanukovych renounced Ukraine's accession plans and replaced them with a policy of non-alignment. Since then, both sides have downgraded their relationship to the Euro-Atlantic Partnership Council. Nevertheless, Ukraine has been the only country to participate in all major NATO-led operations and missions intended to enhance interoperability with foreign militaries. At this stage, Ukrainian national contingents contribute to NATO's train and advise Resolute Support Mission (RSM) in Afghanistan and the multinational NATO forces (KFOR) in Kosovo. Likewise, Ukraine provides support for NATO's naval operation "Active Endeavour."

NATO's response to the crisis in Ukraine

In 2014, Pro-Russian gunmen took over Donetsk, Luhansk, and other towns and cities in the Donbas region of eastern Ukraine in April and May. According to many observers, the weakness of Ukrainian forces was due to many factors, including poor training and morale, shortages of key equipment, and incompetence in the military and police command. Thus, there was an urgent need for the Ukrainian government and NATO to act.

In the early stages of the crisis, dialogue commenced under provisions of the NATO-Ukraine Distinctive Partnership, and allied as well as Ukrainian representatives met at NATO HQ in Brussels on 1 April 2014. They pledged to implement "immediate and longer-term measures in

order to strengthen Ukraine's ability to provide for its own security," with stress on support for comprehensive reform in the security and defence sector.

Among such measures belong a number of programmes and activities in support of Ukraine. For a brief illustration, the NATO Science for Peace and Security Programme was developed, which includes several workshops and training courses in a number of fields. Also, the Defence Education Enhancement Programme was created to advise Ukrainian academics from defence education institutions. Then, the NATO's Building Integrity Programme was developed to Ukraine's defence and security institutions to strengthen their integrity, transparency and accountability and reduce the risk of corruption. A major milestone was achieved in September 2015 in agreeing the NATO-Ukraine Strategic Communications Partnership Roadmap. Last but not least, the NATO's Professional Development Programme was put forward to train key civilian security and defence officials on effective democratic management and building local capacity. After the September 2014 Wales Summit, NATO Allies have established five Trust Funds for the-Command, Control, Communications and Computers (C4), the Logistics and Standardization, Cyber Defence, Military Career Management and the Medical Rehabilitation. Most recently, following the NATO Warsaw Summit in July 2016, a Comprehensive Assistance Package (CAP) was endorsed to further consolidate and enhance NATO's assistance for Ukraine.

What is more, the Alliance's Partners have been trying to improve the situation inside Ukraine. The European Union has contributed over € 279 million in humanitarian and early recovery aid to the most vulnerable since the beginning of the crisis. The OSCE personnel deployed in Ukraine has been trying to guide the Ukrainian authorities to follow all the necessary rules in order to comply with the international law standards. Nevertheless, there is still a need for NATO and its partners to keep cautiously demonstrating solidarity with Ukraine in order to help the country to resolve the crisis and achieve permanent stability.

Bright future?

In the present situation, it is uncertain whether NATO states are prepared to fight for Ukraine. But there is an opportunity for the Alliance and its Partners to improve the focus and effectiveness of support for Ukraine in capacity building.

Policy Recommendations

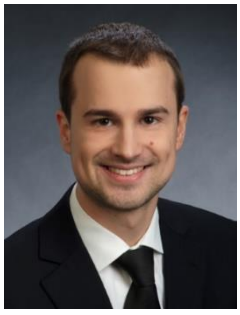
1. Bolster the policing, surveillance and electronic warfare capabilities of the Ukrainian state in order to pre-empt further escalation of military activity by rebel groups
2. Continue engagement in providing advisory and financial support in crucial areas
3. Help to reshape the economic structures of Ukraine.

Miroslava Grausová is an undergraduate student of the International Relations and European Studies at the Metropolitan University of Prague, currently undertaking a study exchange program at the Faculty of International Relations at the Institut d'études politiques de Lille (Sciences Po Lille). During this year's summer period, she was a part of the European Centre of Diplomacy and Peace in Warsaw, Poland. There, she underwent the Training of the Future Diplomats program. This exceptional experience further strengthened her committment and

interest in Security studies, NATO's work in particular, as the training was conducted in Warsaw, the epicentre of the NATO's 2016 Summit .Over past few years, she has lived in many countries, what contributed to her open-mindedness and personal development. She set off for London at the age of 18, in 2013. The following year she went to live in France. The summer 2015 she lived in Greece. This year I have lived in 4 countries: Slovakia, Czech Republic, Poland and currently France. She believes to be a good future "asset" to help the international community, in any possible way which she needs to find and define.

It's the Economy, NATO!

Kamil Klosek



Operation Unified Protector in Libya has entailed unintended consequences with which local and external actors have to cope until today. Whereas the intervention was not the "primary" cause for the following low-level insurgency and political division within Libya, the intervention facilitated this development due to the following reasons. First, the defeat of Qaddafi's security forces led to a power vacuum in certain parts of the country. Civilian rebels and defecting parts of the regular army did not control the entire territory of Libya under a unified command. Second, the Libyan economy experienced a tremendous economic breakdown in 2011, a partial recovery in 2012 and then again plummeted in 2013/14. In a country with a high share of young people, these income shocks unsettled economic relationships, increased unemployment and hence lowered opportunity costs to join local militias. Third, there was dissatisfaction inside the population over the new leadership of Prime Minister Ali Zeidan. Post-revolution economic recovery in 2012 did not reach ordinary citizens who felt that corrupt elites are dividing the cake of oil export revenues among themselves and that the leadership was not able to control the security situation inside the country. Fourth, the tremendous dependence of Libya on oil exports[1] meant that the primary possibility for Libyan people to increase their wealth was to seek rents from the oil economy. Those who controlled oil fields, pipelines and ports were those who could obtain indispensable cash in an otherwise weak economy. The following four policy recommendations can be extrapolated from the intervention in Libya for other post-intervention scenarios.

First, NATO should be put into position of controlling export sites at borders or ports in a post-intervention country in order to ensure a stable out- and inflow of goods (and people). Countries need export revenues to accrue foreign currencies in order to pay for goods that are not available through domestic production. During civil wars, profitable economic sectors are targeted and either destroyed for strategic purposes or fought over by local warlords/militias. With this strategy, NATO could ensure that the legitimate representatives of the post-intervention states are able to collect "their" taxes and royalties and prevent local strongmen from profiting from illicit trade. In addition, such a strategy would make it more challenging for foreign fighters to enter the post-intervention country. This requires an adequate UN mandate or the invitation by the legitimate

government of the post-intervention country. It can also be implemented in collaboration with neighboring countries.

Second, NATO's crisis management should include the protection of natural resource extraction sites so that local militias do not compete for access violently. Whereas the first point pertains to external (trade) relationships of the targeted country, this argument focuses on the domestic situation. In a post-intervention environment, it has to be expected that certain actors will try to gain access to natural resource extraction sites (or their infrastructure) as they often constitute the only means to generate revenue since manufacturing industries are frequently disrupted in civil wars and cannot be rebuilt quickly. Such a policy can be executed in collaboration with trained loyal local forces in order to increase legitimization of deployed NATO personnel inside the post-intervention country.

Third, in a post-intervention environment NATO has to assist the new legitimate government in maintaining security for a short-term period, but military and policing support cannot be a "free lunch". In exchange for support, the new domestic leaders have to be pressured to abstain from corruption as it alienates the population. Economic recovery programs and quick economic reforms, which allow local people to engage in trade, as well as the protection of property rights have to be pursued in order to allow the civilian population to create income improvements outside the security sector and also attract green field foreign direct investment. The window of opportunity is short since the new government can entrench itself over a middle range period (1-2 years) and become indispensable to outside actors in keeping prima facie stability until the next civil war erupts. Such a government is less amenable for outside pressure.

Fourth, during the intervention period NATO should abstain from targeting key natural resource extraction sites, especially in the oil and gas sector, because crucial revenues for investments will be missing in the post-intervention state and people will fight over the remaining "cake" that has not been destroyed. It is tempting to think that the removal of financial income will lead to a faster demise of the targeted faction, however, one should remember Clausewitz who pointed out that a full-scale war should not be conducted since we have to deal with post-war conditions. Rebuilding efforts often require the involvement of foreign companies which in turn have leverage over the post-intervention government. Lack of expertise, brain-draining movements during the civil war and a shattered infrastructure can lead to unequal bargaining relationships between companies and a newly established government to the detriment of the local population.

<u>Policy Recommendations</u>

1. NATO should control or supervise export sites at borders or ports in a post-intervention country.
2. NATO's crisis management should include the protection of natural resource extraction sites so that local militias do not compete for access violently.
3. For a short-term period, NATO has to assist the new legitimate government in maintaining security, but military and policing support cannot be a "free lunch".
4. During the intervention period NATO should abstain from targeting key natural resource extraction sites.

Kamil Klosek was born in Poland, but has lived the majority of his life in Germany. He lived close to Karlsruhe and after high-school went for his Bachelor degree in Political Science to the University of Mannheim (including one semester at the University of Malta). He then completed his Master double-degree in International Conflict Management and Security Studies at the University of Konstanz and Charles University in Prague. He decided to continue his PhD about the nexus between civil wars, foreign interventions and natural resources at Charles University and currently he is in his second year of doctoral studies. His working experiences include being research assistant and research interviewer, co-teaching the course "Regional Security Studies" at Charles University, as well as project based involvement and business related employment. He is also blogging on his website outsidecivilwars.org about thoughts regarding civil wars.

Article 5 alone is not enough – why NATO still needs a military crisis and conflict management capability

Eva Mattes

At the Warsaw Summit 2016, NATO reconfirmed its refocus on Article 5, putting deterrence and collective defense on the spotlight. At the same time, NATO experiences a declining willingness of member states to commit to long term military operations in crisis and conflict areas. These two aspects combined seem to result in a de facto standstill of NATO's ability to provide an active contribution to the world's crisis and conflict management. Furthermore, shifting the focus on Article 5 prohibits NATO from prospectively obviate past mistakes from latest stabilization and counterinsurgency (COIN) operations in order to improve the Alliance's strategic concept. Moreover, it withholds the risk of losing specific knowledge and expertise gained on how to run stabilization and COIN operations within the context of a comprehensive approach. Due to this development it is of essential importance for NATO to preserve lessons identified and learned as well as structures, (non-kinetic) capabilities and networks and to restore the willingness of member states to commit themselves to actively participate in NATO's crisis and conflict management.

The current world consists of various failed states fostering the development of local and regional terrorism and refugees, looking at examples such as Syria, where local military groups are not able to detain ISIS from capturing cities, enslaving their inhabitants and forcing survivors to flee their country. Consequently, NATO's ability and willingness to engage in respective regions is essential for the world's ability to deal with these areas of crisis and instability in general. As NATO members cannot agree on joint military measures and the Alliance mainly focuses on Russia, they rely on so called "coalition of the willing" when it comes to crisis and conflict management. The reflex of the Alliance to regain internal political unity by emphasizing the Article 5 commitment after the Afghanistan experience is reasonable. Even more if one bears the Russian annexation of Crimea

and the Ukraine conflict in mind. Nevertheless, the need for crisis management does not decrease but increase, looking at the recent examples of Libya, Syria or Mali. These developments indicate, in a broader perspective, a fundamental obstacle NATO is facing in maintaining the effectiveness and credibility of Alliance as the biggest security and defense organization worldwide.

As said, NATO's concept of refocusing on Article 5 seems to be a reasonable decision at first sight, but carries a wide range of consequences. Among these is the aspect that the vast majority of the Alliance's member states maintain only a "single set of forces". Strengthen their kinetic capabilities in the scope of an Article 5 scenario means consequently to reduce the non-kinetic abilities simultaneously as governments are still reluctant to increase the investments for the armed forces overall. Nevertheless, non-kinetic capabilities are key to successful crisis management and are needed for a variety of measures such as supporting the stability of the host country, the security of its population and its government, as well as coordinating military and civilian activities. Moreover, within the NATO Command and Force Structure skill sets, staffs and knowledge gained during the past decade in the area for crisis management operations most likely will either not be maintained or no longer be improved.

Furthermore, freezing up all cooperation between NATO and Russia is going to have a serious impact on crisis management as well. Generally speaking, NATO is more dependent on partnerships and cooperative acting than ever. Examples of Ukraine and Syria proof that NATO members seem hesitant to get militarily involved. Non-coercive options of diplomacy or instruments like the OSCE are indisputably the number one choice, but can be ineffective against criminal terroristic organizations or state terrorism. Alternative options to a UN or NATO mandate such as "coalitions of the willing" can offer additional support, but need substantial diplomatic efforts to be set up, and misses out on any of NATO's advantages. Moreover, on a political level a military organization, de facto unwilling to commit to military operations, upholds no power or persuasiveness.

Summing up, as the world is in great need for crisis management, NATO cannot back down on its responsibility of managing crisis and conflicts, even in terms of an enlarged collective defense strategy. Future core task must therefore be managing, on one hand the pursuit of its collective defense strategy, on the other hand preserving lessons learned, structures, capabilities and staff of crisis management missions. Considering the worlds current conflicts, a complete retreat to Article 5 would mean a step back within NATO's evolution process in the aftermath of the Cold War area.

<u>Policy Recommendations</u>

1. The Alliance is well advised to maintain a military response capability
    a. to protect the territory of its member states
    b. to run crisis and conflict management operations.
2. NATO strongly needs to enlarge its cooperation with other countries and cooperation.
3. Especially and in any cases, NATO must remain to work on its diplomatic ties to Russia.

Eva Mattes has been majoring in Political Science at the Ruprecht-Karls University in Heidelberg since October 2015. In 2015 she completed an internship at the German Atlantic Association in Berlin. Organizing discussions and talks on international security issues, she is a member of the

Forum for international Security Heidelberg. Moreover, she is part of a team organizing the 29. Heidelberger Symposium, an interdisciplinary student initiative. Currently she is working as a student assistant as part of a project concerning diffusion, learning, and cooperation in managing transnational conflicts. Her academic interests focus on international relations as well as foreign and security policy.

NATO's future role in crisis management

Dániel Paschek

Since NATO is a creation of the cold war rivalry after the fall of the Soviet Union, the alliance could have lost its purpose. It did not, but thanks to several factors, such as the changed world political and economic situation, to the intensifying effects of globalization and the appearance of new relevant factors such as NGOs, internationally operating terror organizations etc. NATO has to reform its operation continuously. In the mentioned circumstances the role of crisis management is increasing significantly, and NATO is taking significant steps to adjust to this ever-changing world. Even though the steps taken to reform are relatively efficient, further steps are inevitable for smooth operation.

Talking about crisis management, one of the most elementary questions is the definition of crisis itself. Even though mostly a crisis is easily recognizable, in this rapidly changing world, a commonly approved definition seems to be indispensable in prospect of efficient crisis management. NATO has a non-approved definition, more of a common understanding of what a situation of crisis is. According to this, a crisis can be understood as "a national or international situation where there is a threat to priority values, interests or goals". This is a good starting point, but in one hand this is not specific enough on the other hand it is not approved commonly.

A lesson drawn from KFOR, is that importance of civilian actors - such as NGOs - importance increased significantly in post-cold war crisis management. Nonetheless the integration of civilian actors in crisis management process is not adequate enough. Consulting platforms should be set up, where significant actors can express their concerns and proposals. Military and civilian organizations should endeavor to plan mission mandates and requirements farther in advance. Joint training should be organized to promote mutual understanding of needs and resource sharing. In addition, mission mandates should make clear the tasks of both military and civilian organizations.

In prospect of crisis prevention, the role of intelligence services and covered actions are getting more and more important. Even though member countries share nationally-gathered intelligence with their Allies, and make them speedily and comprehensively available to NATO Headquarters and major NATO commanders, there is no own sources of intelligence in peacetime. This fact

makes prevention and crisis management planning less smooth. A common intelligence service seems to be impossible, but wider intelligence cooperation is highly important in prospect of future crisis management. This is why a coordinating office should be set up for the harmonization of national intelligence services.

Even though, the question of interoperability is an evergreen case in debates, NATO should emphasize more the importance of weapon and equipment standardization. In prospect of cost-effectiveness this should be accomplish, by a policy controlling the new military acquisitions. Beside the actually existing concepts, doctrines and procedures promoting interchangeability and interoperability NATO should stress the importance of standardized weaponry.

Last but not least, NATO should have an emergency defense budget increase mechanism. The logic of this policy is that NATO members should feel safe without a huge amount of military spending. Besides the nuclear umbrella, they could be aware of the fact, that in case they got threatened by anyone, the other members of the alliance will increase their defense budget parallel with them. The inequality in military spending – even compared to GDP – is having a negative effect on the cohesion of member states as its also boosts mistrust. Threatened countries should feel the support of their allies and should be able to trigger this mechanism, initiate the increase of defense spending of countries not reaching the 2% limit of military spending. To set an example, those countries triggering the mechanism should increase their defense spending first. Countries under 2% of military spending should be obligated to increase their defense budgets by a certain percentage of the initiators defense budget increase, depending on their economic development.

Policy Recommendations

1. NATO should create a specific and commonly approved definition of crisis.
2. NATO should concentrate much more on the integration of civilian actors into the crisis management process, with consulting platforms, joint trainings, and broader mandates.
3. NATO should create a coordinating office for the better coordination and information sharing of national intelligence services.
4. NATO should stress the importance of standardized weaponry in case of new weapon acquisitions
5. NATO should have a so-called emergency defense budget increase mechanism.

Dániel Paschek is a MA student of Corvinus University Budapest, specializing in diplomacy on the faculty of international relations. Besides my University studies, he is the chairman of the Association of Diplomacy in Practice. Since he is very much committed to the promotion of international understanding, and European values, he initiated several changes in the life of the organization, for instance, he started an international opening. The organization started to build a strong network of foreign associations with similar goals to theirs. They participated in several international projects, and started to organize a series of conferences. The main goal of these events is to create and deepen an understanding approach among the European nations.

Preparing for Crisis Response Operations in an Evolving Information Environment

Stéphanie Poulin (@PoulinStef)

In an increasingly complex security environment, not only have lines between peace and war blurred, but also complex and multidimensional security threats have emerged at the periphery of the NATO and its partner countries. The information environment, characterized by a continuous flow of information and an active social network of interconnected audiences, greatly affects the perception and understanding of NATO's activities beyond the borders of its member countries. In the context of intervention fatigue after protracted engagements in Iraq and Afghanistan, and the necessity for most NATO members to do more with less, it is critical for the Alliance to develop appropriate, timely and accurate communications with key audiences to gain support for continuing NATO crisis response efforts. Despite the growing interest in strategic communications, it remains a relatively underdeveloped field in its early stages of development, for NATO and its member countries.

The rise of complex transnational threats and the unlikelihood of traditional aggression make non-Article 5 NATO crisis response operations more likely in the foreseeable future. At the same time, operations not falling under NATO's principle of collective defence do not require the Alliance to move as a whole. Nations are sovereign in deciding which missions they want to be part of. This has the unintended effect of eroding member solidarity and the sense of collective belonging, allowing countries to prioritize individual national threats over common threats to the Alliance. In addition, misinformation has reinforced the perception that NATO is driven by military interests, and controlled by the United States under an alleged façade of democracy and freedom. However, cohesive and strategic messaging is crucial for NATO's crisis response operations, since strong support from all member states and their populations remains the foundation for their success. Therefore, the mentioned issues must be addressed beforehand of operations through appropriate policy and strategic-level concepts.

Over the last ten years, NATO has conducted crisis response operations in seven non-member countries: Bosnia and Herzegovina, Afghanistan, Iraq, Pakistan, Sudan, Somalia, and Libya, as well as off the Horn of Africa. NATO must engage not only with the populations of the 28 member countries, but also with those in partner nations, those in countries where operations unfold. The more partners and audiences there are, the harder it is to agree quickly on messages and to coherently communicate them.

Empowering more personnel to communicate through words, videos or imagery will enable NATO to rapidly engage on current events. This also helps develop a sense of proximity between audiences and organizations. Messages must address negative perceptions and attitudes to gain support and dissipate doubts and reluctance. Tailoring messages is an effective way to reach audiences, to create trust and credibility and should include awareness of cultural and linguistic specificities of the local populations who are strangers to NATO forces. NATO must have a

compelling, easily understood and consistent narrative without hampering local initiatives of outreach.

It is better for NATO to be proactive in explaining the aims of operations than to have to spend energy and resources to correct misinformation. Often, it is even impossible to undo misperceptions created by the media. Therefore, NATO must become the first source of information about its operations. In a world where what is said or not said has an impact on societies and social groups, NATO's best option is to take the lead on creating the narrative and the desired information effect.

Communications is one dimension NATO has been neglecting over recent decades. This has created a gap between the Alliance and the populations it serves. Creating an environment in which NATO's populations understand and support the aims of the organization has become essential. By taking adequate measures, the organization can close this gap and enhance support of its political and military objectives.

Policy Recommendations

1. NATO must recognize "influence" as a non-military strategic threat for its stability and cohesion and reinforce the sense of belonging and common spirit at the population level by transitioning messaging from military to human.
2. NATO must train communications officers at all level to efficiently deliver tailored messages through the right channel while taking into account cultural contexts.
3. More resources must be allotted to reinforce communications and outreach activities with audiences where NATO conducts operations or may conduct operations in the future, including the Middle East, Africa, and Asia.
4. Strategic communications must be developed in concurrence with operational plans in preparation and during early stages of crisis management for humanitarian or military operations.

---

[1] Around 80% of the total export value was constituted by crude oil in 2014 according to UN Comtrade and BACI estimates

Stéphanie Poulin currently works for the Department of National Defence of Canada as a Communications Officer. She has previously worked for Global Affairs Canada and provided support to the Canadian Permanent Representation for the Organisation for the Prohibition of Chemical Weapons (OPCW). Her expertise lies in Euro-Atlantic security, threat perception, security in Northeast Asia, and communications and issues management. In her thinking, she includes/uses non-traditional approaches and explores new avenues to address emerging security issues. She holds an MA in International Studies with a focus on multilateral disarmament and chemical weapons from Université de Montréal, Canada. She also completed a BA in History.

What needs to change in NATO's decision-making in a crisis?

Carina Soares

Any crisis could be a serious threat to the basic structures or to the fundamental values of a society. Its complexity is enlarged by the necessity to make vital decisions in a short time. A crisis can be political, military, humanitarian, and natural or even be a consequence of technological disruptions. Especially in these difficult times, a successful and effective Alliance depends on the contribution of their citizens. The more the public knows about NATO operations and how member states contribute to the Alliance, the easier it is for citizens to encourage their governments to maintain high levels of involvement. Activities and associations like the YATAs are significant ways for the civilians to recognize respect and experience NATO. By increasing transparency to the public, NATO could increase the feeling of togetherness and create important shared values.

The world is changing and the post-cold war security paradigms are no longer adequate to explain the rapid transformation of the world. The emerging and suicidal terrorism, the natural hazards and the civil wars break with the past and show that it is necessary to reform the national and international security conceptions to respond to these crises. One of the fundamental security tasks of NATO, which can include military and non-military measures, is exactly the management of such crises.

As all these crises can happen without being predicted and as they affect the normal function of basic infrastructures, NATO tries to act in these complex security environments, employing a mix of political and military tools to manage crises that can be a threat to the security of the Alliance's populations.

At the beginning, NATO had only the capacity to deal with crises related with collective defence (Article 5), but during the 1990s NATO participated in and launched out-of-area-operations, which were not included in the Article 5 sphere, in non-NATO member states in order to protect civilians at risk and prevent those crises from destabilizing the region. Missions like KFOR in the Balkans represented this new approach to security in the Alliance and the more multidimensional mission than during the Cold War. However, this idea of expanding capabilities and areas of intervention can give a bad image of NATO, mainly because the term "crisis" has not a concrete definition within the Alliance, which allows the North Atlantic Council (NAC) to have a huge flexibility in deciding when a situation becomes a crisis and to make decisions that represent too obviously the national interests of its member states.

The allies decide on a case-by-case basis and by consensus when discussing a crisis. This decision-making process is founded on Article 4 that affirms the necessity of the allies to consult together, when one considers that any of the parties is being threatened. This consultation procedure is important in the complex security environment of today's world.

The KFOR mission in the Balkans is a lesson of the necessity for NATO to adapt its policy and procedures to ensure the effectivity of its operations and to stop the idea of NATO "intervention

fatigue". The rule of consensus within NAC makes the decision-making process too obsolete and difficult to achieve. As studies have shown, in moments of lack of time and immediate threat to human lives, the capability of negotiation parties to act in a rational and effective manner is decreasing. Hence, it is also necessary to have more transparency within NAC because it helps in moments of stress, ambiguity and complexity, this means, during a crisis. If civilians could track what is being discussed and decided within NATO, during a crisis, the public opinion could help to solve a crisis and to reach a decision in an easier way. The transparency in the function of the organization would make the civilians feel that they really belong to NATO and that their opinion is heard.

As one of the problems of NATO, that decreases the effectiveness of its operations, is the process and the dynamics of decision-making and as no decisions on planning, deployment or employment of military forces are taken without political authorization, the following recommendations could improve NATO operations success:

Policy Recommendations

1. Improve internal dynamics by implementing an advisory vote system and more transparency. Transparency is the key to a value-oriented organization and a necessary condition for creating trust among the civilians. (Broadcast live sessions of NAC, online conversation with the public; make access to information easier, etc.).
2. Improve the importance of the regional interests, within NATO, to increase commitment (overcome the idea of the difficulty to achieve consensus because of national interests).

Carina Soares studies in Lisbon, but is original from a village from the north of Portugal. Carina has a bachelor degree in International Relations and she's now doing a postgraduation programme in Security, Globalization and Diplomacy. Her interest in security started in the first year of bachelor, but mainly in her Erasmus semester in a german university in Nuremberg. This year, she joined the YATA Portugal Executive Board and organized the summer seminar of YATA Portugal in Lisbon with a focus on the Warsaw Era and the idea of collectively defending the Alliance. This is Carina's first participation in one YATA seminar outside Portugal and she hopes that it would be the first of many others.

Breaking the arc of crisis and preventing future ones: NATO's crisis management on trial

Christian Zrenner

The current waves of insecurity reflected in Russia's expansionist politics in the East and by a zone of failing or failed states in the South, originating from Libya to Afghanistan, being a breeding ground for jihadist terrorism by al-Qaeda and the self-proclaimed "Islamic State" and massive migrant flows have created an "Arc of Crisis" stretching alongside the borders of European NATO-member states. In response to similar patterns of instability, NATO had been pursuing

high-profile military-crisis management operations in the past, such as the one conducted by NATO's Kosovo Force (KFOR) in the Balkans as well as ISAF and Resolute Support Mission in Afghanistan. Though often regarded as stand-alone by politicians, these operations must be seen in a broader context given the indivisibility of security threats and their propensity to cause spill over and cascade effects. Therefore those operations have and will unequivocally challenge the Alliance`s crisis management efforts in order to deal effectively with them. On the other hand, especially the improved security situation in Kosovo shows that the Alliance is able to stabilize post-conflict situations and to support reconstruction efforts.

The post-conflict situations in the Balkans, Iraq and Afghanistan have shown that the usefulness of military power alone for sustainable stability has serious limitations. In order to guarantee effective crisis management in the long term, civilian instruments like police forces, judges or civil administrators are of crucial importance. First mentioned in NATO's Strategic Concept from 1991, the alliance has been seeking to enhance the integration of civilian instruments through civil emergency planning, i.e. the coordination of the Allies' national planning activities ever since. However, civilian planning and assets strictly remain under national control and there are often problems of internal coordination between the respective national ministries. National stabilization and reconstruction capabilities are rarely organized into deployable assets that can provide cohesive, effective response options and often assembled in an ad hoc manner. In places like Afghanistan, the lack of civilian capabilities required NATO troops to take over civilian tasks. This is problematic, since it can lead to a perceived militarization of civilian instruments. Therefore NATO needs to improve civil-military cooperation with partners, international organizations, nongovernmental organizations (NGOs), and international organizations, in particular with the EU and the United Nations (UN).

Another lesson to be learned especially from ISAF is that the importance of the development of professional, capable and self-sustaining national security forces must be at the heart of missions with the objective to stabilize post-conflict situations. Referring to the situation in Afghanistan, the success of these efforts remains doubtful. Beside the Afghan National Army (ANA), the main providers of security are the Afghan National Police (ANP) as well as the Afghan Local Police (ALP) - at least in theory. If they, however, lack the trust of allies and the local population by not improving local security and curbing the influence of the Taliban but collaborating with the enemy or conducting ill-treatment of the population, their empowering could benefit the dissatisfaction with the Afghan government and give rise to new violence.

In order to improve cooperation and hereby redefining NATOs role in conflict prevention, crisis management, and post-crisis follow-up, the implementation of the following propositions is recommended:

Policy Recommendations

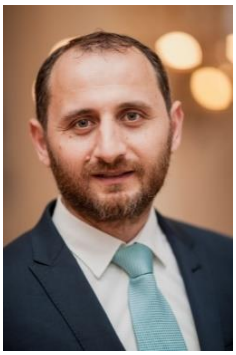
1. Civil-military cooperation in planning should be lifted to another level through an EU-NATO cooperation agreement. Such an agreement would provide for full involvement of the EU in planning for scenarios in which NATO would lead a military operation and the EU would lead a concurrent civilian deployment.

2. More cross-representation at the strategic-military and operational levels is required to ensure that civilian viewpoints are taken into account in NATO's planning processes ultimately facilitating civil-military coordination at the operational level. The Civil Military Planning Directorate, EU's new civil-military planning body, could become a platform for increased cooperation.
3. Professional training as well as successful operations of national police forces should be ensured by provision of sufficient numbers of police instructors as well as by a guarantee of appropriate payment in the short, middle and long-term. This prevents desertion to insurgents and helps maintaining the provision of government services especially in vulnerable parts of states.

Enlargement, enablement, entrapment? NATO's future approach to cooperative security

When policy makers and experts address the numerous challenges NATO faces today outside of its members' territory, security part-nerships and defense capacity building are core instruments to pre-vent resource-intense and domestically contested out-of-area opera-tions. Yet, they allow the alliance's members to further maintain or even enhance their influence on peripheral states, containing there-fore transnational security risks and destabilization. In times, where NATO's Open Door policy seems to have reached its limits, has ena-blement become the new enlargement? What does this mean for new members of the alliance such as Montenegro or traditional pil-lars of cooperative security such as Israel? Can mutual expectations be harmonized or is a „two-class"-system of security inevitable?

Panelists



Shalva Dzidziguri is a Research Fellow at the Georgian Center for Security and Development and Fellow of the Mercator Program Center for International Affairs (MPC) GmbH. His area of expertise includes conflict resolution, transatlantic security issues as well as NATO enlargement and peacekeeping missions. Previously, he worked for the NATO Parliamentary Assembly in Brussels and as Partnership for Peace (PfP) Research Fellow at the NATO Defense College in Rome. As a Georgian Army Peacekeeper, he was deployed to Baqubah, Iraq (2004-2005) and was awarded the Certificate of Appreciation for Noble and Meritorious Service in Peacekeeping Operations. Shalva is an alumnus of the Young Atlanticist Working Group at the Atlantic Council in the United States and a member of NATO's Future Alumni Network. Shalva holds an M.A. from the Central European University focusing on International Relations and European Studies.

James H. Mackey is Head of the Office of Euro-Atlantic and Global Partnership in the Political Affairs and Security Policy Division at NATO Headquarters. In this capacity, he is responsible for overseeing NATO's relationship with partner countries in Western Europe, the Western Balkans, the South Caucasus, Central Asia, the Asia Pacific, Africa, and Latin America. Before assuming this position in 2011, Mr. Mackey served for seven years as an officer in the Political Affairs and Security Policy Division at NATO, where he was responsible for NATO's bilateral relations with a number of partner countries, including Georgia, Serbia, Moldova, Belarus, Bosnia and Herzegovina, and Kyrgyzstan. In 2010, he was detailed to the Private Office of the Secretary General to conduct a reform of the NATO intelligence-sharing process. Mr. Mackey is a former Luce Scholar, and spent 2000-2001

teaching international relations theory at the Beijing Foreign Affairs College. He holds a Bachelor of Arts in Politics from Princeton University and a Master of Arts in Law and Diplomacy from the Fletcher School of Law and Diplomacy.

Capt (N) Arvi Tavaila is the Finnish Defence Attaché for Germany, Austria and Hungary. Prior to coming to Berlin, he was stationed as the DACOS Operations with the Finnish Navy Command. He also served as a Battalion Commander of the Uusimaa Brigade, Ekenäs Coastal Battalion and as a Staff Officer with the Finnish Defence Command and the Ministry of Defence where he worked the NATO desk. His international experience includes two deployments with IFOR and SFOr to Bosnia as well as to the NATO HQ in Brussels.

Introduction and Moderation

Sebastian Feyock has been a program officer with the USA / Transatlantic Relations program since February 2012. He coordinates the Transatlantic Round Table. From August 2013 until July 2015, he also worked as a program officer with DGAP's `Future Forum Berlin'. Prior to joining DGAP, Sebastian worked as a project assistant for the BMW-Foundation Herbert Quandt and the Tönissteiner Kreis e.V. and freelanced as a project and research assistant for several institutions. In 2009 he spent three months at the Stockholm International Peace Research Institute (SIPRI). Sebastian regularly appears on national and international media, commenting on German and U.S. foreign and security policy. His research focusses on maritime security. Since March of 2016, Sebastian is a member of the board of the Youth Atlantic Treaty Association (YATA) Germany. In April 2015 he was selected into the think tank "Young Professionals in Security Policy" of the Federal Academy for Security Policy (BAKS). From 2011 to 2014, he was a member of the board of the German Association for Peace and Conflict Studies (AFK). Sebastian studied political science and philosophy in Greifswald and received an M.A. in Peace and Conflict Studies from the Philipps-University Marburg.

Young Leaders

Amigos in unchartered waters: A continental strategy for NATO's reach to South America

Robert Helbig

NATO is very busy these days: hybrid warfare, terrorism, maritime security – rapid response, resolute support, reconnaissance. It is hard to blame the Alliance focusing on its immediate threats, but it would be shortsighted to neglect the value of cooperative security as one of its core tasks: to build security through military cooperation across the globe. One region in the world constantly neglected by NATO policy makers is South America, although partnerships would have much to offer, from building regional capacity for transnational threats to mission support to advancing international legitimacy. Given the continent's political reorientation, it is time to explore possibilities for cooperating with NATO's natural partners in the South.

None of the Alliance's over forty partners is situated in South America. The Alliance's relations with the continent are sparse, often from the past and mostly military-to-military. For example, Peru has signed on to NATO's codification system. Brazil has hosted workshops of the NATO Defense College. Chile and Argentina have participated in NATO's Bosnia operation. While not directly in South America, neighboring El Salvador even provided support in Afghanistan. Colombia engages in political consultations with the Alliance, trained with NATO at the Horn of Africa, and established a liaison at NATO's military headquarters SHAPE to coordinate initiatives from building integrity to information sharing.

These contacts should serve as a starting point to broaden and deepen cooperation on the basis of mutual interest: It should be NATO's goal to assist South American states building capabilities to combat threats that may affect the Alliance, such as drug trafficking and piracy. Building political trust and military contacts, the Alliance could pave the way for South American states to participate in NATO-led missions. If this seems too farfetched, NATO could at least use the chance to do away with its stigma of being a Cold War relic and arm of American imperialism.

Similarly, South American states could benefit by gaining capabilities, especially expertise in interoperability and experiences in peace operations, which would help enable them to advance their role in international security. Institutional relations with NATO would also help governments to lobby for their view of world politics, often neglected in international fora.

Political differences between South American countries and the North Atlantic Alliance have suppressed most dialogue between the parties in the past. But the region is currently reorienting itself in the wake of an economic downturn and a shift away from populist governments, such as in Argentina and possibly even in Venezuela.

For the first time since 2003, the regional leader Brazil is interested in constructive engagement with "the West," having realized that its competitive strategy with the US has its limits. But even

before – under former President Dilma Rousseff – Brasília has been tilting back towards the US and Europe as a result of a massive economic crisis, triggered by a lack of reforms, shrinking commodity prices and political turmoil in the wake of a unmatched corruption scandal. Thus, Brazil's reorientation on the international stage is not merely political, but structural.

One can witness very different, but equally positive, developments in Colombia. Although the October 2016 referendum about the deal to end a 52 yearlong war between the government and the FARC did not pass, the parties remain committed to peace. Colombia continues to prepare itself to become an external security provider, establishing a diplomatic profile and redefining the mission of its military, eager to share their experiences in insurgency warfare. Of course, the country faces many challenges implementing a possible agreement – from land reform to establishing the rule of law in currently ungoverned spaces – but senior Defense Ministry officials already insist that the partnership with NATO is one of Colombia's highest strategic goals in the post-conflict environment.

Given this background, NATO could proceed to deepen and widen its relations in the region in a three-stage program:

- Deepen relations with Colombia, establishing a trust fund to support post-conflict force transformation, improving interoperability and building capabilities for partaking in international peace operations.
- Invite Brazil to participate in uncontroversial military-to-military cooperation, for example to assist NATO in the Aegean Sea with the specific focus on rescuing refugees, possibly utilizing Brazil's resources from its activities in the nearby UNIFIL mission off the coast of Lebanon. This initiative or any other military-to-military activities could serve to open the door for political dialogue.
- Build trust by inviting the newly elected governments of Argentina and Peru, as well as Chile, to consult on security concerns, while offering dialogue with NATO critics in Venezuela, Bolivia and Ecuador to discuss sensitive concerns, such as the Alliance's cooperation with Colombia, in a track II diplomacy format.

Although opportunities for cooperation are plentiful, teaming up with South American governments can be frustrating because of a different understanding of sovereignty routed in a colonial past. Therefore, this paper does not suggest NATO taking a pro-active role in shaping regional security structures (such as UNASUR, actually established to contain US influence on the continent), but to invest in pointed bilateral trust-building measures. If the HQ is busy managing peace at Europe's borders, other NATO bodies could reach out, say the Parliamentary Assembly, Defense College or Allied Command Transformation.

The reverse of the Pink Tide – the turn to the left – is a unique moment for NATO to broaden its cooperation portfolio with democratic states, influential in the Global South, rich in experiences in internal conflicts, and eager to develop their role on the diplomatic stage. Arguably, it is not easy to learn dancing samba, salsa and tango, but one does not know what he is missing out if he has not tried.

Policy Recommendations

1. As South America is reorienting itself in the wake of an economic downturn and a shift away from populist governments, NATO should use the possibility to reach out to its natural partners in the South
2. NATO should assist Colombia in transforming its forces and invite Brazil to participating in uncontroversial military-to-military cooperation.
3. NATO must offer a political dialogue to the newly elected governments of Argentina and Peru.

Robert Helbig is a PhD student with a focus on NATO's global relationships at the University of the Federal Armed Forces in Munich. He holds a Master of Arts in Law and Diplomacy from The Fletcher School at Tufts University where he specialized in international security policy and business. In addition to his work and research activities in the Post-Soviet Space and Latin America, he has served as a Carlo-Schmid-Fellow in the Emerging Security Challenges Division at the NATO Headquarters during the height of the Ukraine crisis. Specializing on NATO's relationships in Asia and South America, Robert has published papers on the Alliance's relations with India, Mongolia and Brazil. His forthcoming policy paper focuses on NATO's evolving partnership with Colombia, to be published at the NATO Defense College in Rome. Robert is also a reserve of the German Army and a passionate skier.

NATO's New Mentality: Cultured Warriors

Roger Hilton (@RogerHilton20)

From the resurgence of great power rivalries to the amplified impact of non-state actors, NATO is facing a hydra of threats. It is a groundswell the Alliance should get used to, as this new global system has de-localized international power with an abundance of increased competition that bears little resemblance to the Cold War order. Consequently, ensuring global security has never been more precarious. Faced with this prospect, NATO would do well to reflect on these geo-political trends to preserve its primacy in the post 9/11 security environment.

Since its inception, the Alliance has shown its adaptation with a more robust Rapid Reaction Forces in the aftermath of the Crimean annexation. While this policy addressed one threatening vector, it is only a half measure in the framework of the global security situation. NATO must accept two truths; they cannot unilateral defend against all threats and future partners and members will be diverse. Consequently, adjustments are needed to NATO's current Strategic Concept "Active Engagement, Modern Defence" that was adopted at the 2010 Lisbon Summit. This undertaking should be anchored by blending NATO's principal of collective defense within the grander concept of cooperative security. To satisfy this, NATO must build its international footprint through cultural exportation and shift its engagement to include more humanitarian missions. Through

these initiatives, it will attract more partners and more critically derive political good will, facilitating more cooperative security. This policy should drive NATO as it will help obtain a competitive advantage over rivals, as well as mitigate episodes of unpredictability. For these reasons, this policy brief will provide feasible ways to build on NATO's current manifesto.

Cultural exportation: Moving forward the Alliance needs to become more sophisticated cultural carriers in person and policy. In response, NATO should advocate weaponizing culture as a means to; influence others, exploit its enemies, and gather intelligence. By consulting anthropologists in policy drafting, it would help NATO produce cross-cultural synergies, notably among non-members like Iraqi Kurdistan or Ethiopia that would help overcome any cultural differences to increase cooperation. To avoid offending locals, understanding how to patrol during Islamic religious festivities or properly search women, would show respectfulness and translate into more trust. This application would also serve to better culturally condition NATO troops, like the Human Terrain System of the U.S. Army, as they enter unfamiliar theatres of war or peace keeping. In the cyber realm, it could be practiced on social media to help win the information war by appealing to hearts and minds of locals. One targeted policy would be making the Norfolk NATO Festival an international circulating event or to hold NATO days in partner states with a cultural Ambassador at its helm.

Partnership Networks: There are a litany of security quagmires outside of NATO's competencies, in areas like migration and food security that directly affect the Alliance. Due to the interconnectedness of issues, NATO should be more pre-emptive in preventing these from avalanching into crises. Similar to its "Berlin Plus" arrangement with the EU, the Alliance must create mirroring enhanced institutional contracts with a range of regional and sub-regional organizations. Raising the level of inter-operability through permanent representations and working groups at organizations such as the; the African Union, International Organization for Migration, l'Union du Maghreb arabe ,Council of the Baltic Sea States, and the Asia-Europe Meeting, would allow for the unobstructed exchange of expertise that would profit the Member States and allies during a variety of security situations. A policy to explore would be a joint OSCE-NATO crisis simulation with a post- result workshop to identify where improvement is needed.

Expanding Competencies: NATO has a proven track record of providing peace support and human relief efforts that have confirmed its competencies outside of a combat role. This strength needs to be further cultivated to reinforce its network of partnerships and to maintain stability. The inferred costs could be financed from national budgets that allocate funds to humanitarian projects, while the new NATO HQ will allow for some of these operations like coordinating logistics to be done from distance. A worthwhile policy would be creating an ad-hoc rapid reaction force of members and partners to engage in humanitarian issues. A timely example would be participating in the construction of migration transit zones in concert with the IOM.

Enlargement: It would be supremely foolish for NATO to disregard its commitment to its Open Door Policy and shun the chance to add valuable new members. Despite the six waves, strategic enlargement should still be revisited based on merit, specifically a commitment to spend 2% of their GDP on defense and uphold democratic values, in the Balkans and Georgia. Specifically a commitment to spend 2% of their GDP on defense and NATO should consider a conditional set

of membership rules for Tbilisi that would preclude them from invoking Article 5 against their occupied territories.

Policy Recommendations

1. NATO must weaponize culture as a means to; influence others, exploit its enemies, and gather intelligence.
2. Similar to its "Berlin Plus" arrangement with the EU, NATO must create mirroring enhanced institutional contracts with a range of regional and sub-regional organizations.
3. NATO must expand its missions more frequently outside of a combat role by creating an ad-hoc rapid reaction force to engage in humanitarian issues.
4. NATO must enlarge with Georgia on a conditional set of membership rules that precludes Tbilisi from invoking Article 5 against their occupied territories.

Roger Hilton is from Canada and an international affairs professional. Roger has previous experience at the Office of the State Minister of Georgia for European and Euro-Atlantic Integration as well as with the delegation of the Kingdom of Belgium at the Organization for Security and Co-Operation in Europe (OSCE). Prior to relocating to Europe, Roger worked as a government and public relations consultant. He is a graduate of the Diplomatic Academy of Vienna where he holds a Masters in Advanced International Studies, as well as a 2013 summer graduate from the Moscow State Institute of International Relations (MGIMO). His research interest include Russian foreign and security policy as well the post-Soviet sphere. Outside of politics, Roger is a French trained chef and founder of a Franco-Nordic catering service in Montreal.

How to build security in an unsecure Europe

Sarah Pagung (@S_Pagung)

The illegal annexation of Crimea brought security challenges right to NATO's doorstep. Russia made clear that it is willing and able to change European borders to pursue its interest. In fact this is not the first time Russia breached the European security order. With its intrusion into the secessionist entities Abkhazia and South Ossetia in 2008 Russia violated the borders of a sovereign state within Europe. The Crimea annexation not only showed Russia's willingness to use military means but also proved its capability to modernize its armed forces. Well-trained and equipped special forces conducted the Crimea operation as part of a complex operational strategy. Russia further displayed its ability to disrupt other states with its cyber attacks on Estonia in 2007 or recently on the German Bundestag. Tensions between NATO members and Russia are not only rising in the cyber sphere but also in traditional military areas. The number of Russian military aircrafts approaching the air space of NATO members has been increasing since 2013. Russia perceives NATO's military manoeuvres in Eastern European member states and the deployment of forces in Poland and the

Baltics as a threat. Due to the lack of trust between NATO and Russia this situation bears the risk of an unintended but highly dangerous escalation.

In response to these threats NATO has to provide security for its members – especially as the OSCE is not able to do so. 40 years after its establishment, the OSCE is not capable to provide a functioning system for conflict prevention and regulation, mainly because the members themselves neglect this role or even the basic principles of the OSCE as it is the case with Russia. In light of the failure of the European security architecture after 1989 NATO will play a crucial role in building security in an unsecure Europe. This includes numerous tasks and challenges, but I want to emphasize three which I believe are of profound strategic importance in achieving long-term security.

First, NATO should not accept new members in Eastern Europe in the near future. This would lead to a decreased security level for all NATO members. Potential new candidates such as Ukraine and Georgia do not have a stable security: Ukraine is fighting a war against separatists supported by the Russian military and Georgia still has two separatist regions supported by Russia on its own territory. Even an integration of one of these countries would transform these conflicts into a direct confrontation between NATO and Russia and therefore increase the risk of war. But NATO should make its position very clear that the decisional-power whether or not Eastern Europe countries will become new NATO members lies only with NATO and these states themselves. Giving Russia a veto right would mean that the strategy of waging proxy wars in these countries is successful and thus increase the risk of further Russian military actions beyond its borders. Therefore NATO should one the one hand maintain the (long term) prospect of membership. One the other hand NATO needs to strengthen the cooperation beneath the membership level, as it is planned in the common declaration of the NATO-Ukraine Commission this summer. Close political and military ties through close coordination, common manoeuvres and transfer of know how are a signal towards Russia that NATO is supporting Ukraine in its struggle for territorial integrity and souvereignty. This souvereignty explicity covers the free choice of alliances. Finland could be model for this: it is not am member, but due to its close ties to NATO and EU not neutral as well. Good Governance and reforms regarding efficiency and transparency should be guidelines for this close cooperation and condition for further support of NATO.

Second, NATO should not further increase or decrease the troop size in its Eastern European member states. The decision to deploy rotating rapid reaction forces in the Baltics and Poland was discussed controversially. German Foreign minister Steinmeier even characterized NATO behavior as sabre rattling. A further deployment of NATO troops in the Baltics and Poland would indeed lead to a decreased security level. It puts the NATO Russia founding act at risk and would strengthen Russia's perception of a threat posed by NATO and could be used by Russia as a justification for more snap exercises and troop deployments in the border region. In fact the Baltics cannot be secured even with more troops due tge so called Suwalki gap. But a decrease of troops would look like a one-sided concession and therefore encourage the Russian strategy. A reduction or withdraw could be a useful bargaining chip in future negotiations.

Third, NATO should strengthen its dialogue with Russia through the NATO-Russia Council. However, NATO members should be aware that this is a long term effort and will not lead to an

immediate consensus on European security with Russia. Still the NATO-Russia council is the best instrument to avoid further unintended escalation. The council should focus on mutual information transfer about manoeuvres and other military exercises and should try to decrease the number of military border provocations. The ongoing Russian deception of its military excerses should be publically condemned by the all Allies. Political and to a lesser extend military pressure are the only levers to force Russia to stick to the common principles. The The Vienna Document or its revision are a usefull guideline. This kind of dialog would help to rebuild trust, which is the necessary basis for future rapprochement.

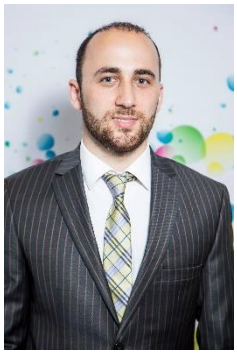
Policy recommendations

1. NATO should not accept new members in Eastern Europe but strengthen its cooperation beneath this level, especially towards Ukraine.
2. NATO deployment in the Baltics and Poland should be seen as a bargaining chip towards Russia.
3. NATO and Russia have to avoid unintended escalation through mutual information in the NATO-Russia Council and trust-building measures in the military sphere.

Sarah Pagung joined the Robert Bosch Center for Central and Eastern Europe, Russia and Central Asia at the German Council on Foreign Relations (DGAP) as a program officer in 2013. She is responsible for the development, organization and moderation of various events with a focus on Russia, the Eastern Partnership and Moldova. Until 2015 she held a position at the Carl Friedrich Goerdeler-Kolleg at the DGAP in addition to her role as a program officer. Since 2016 she is working as a freelance lecturer at the Freie Universität Berlin where she is holding seminars on Eastern European politics. In 2012–13 she participated in the European Voluntary Service's German-Russian exchange program in Saint Petersburg – working in youth and adult education. Ms. Pagung studied political science at the Freie Universität Berlin and is currently writing her PhD thesis on Russian information policies in Germany.

America between keeping the Euro-Atlantic marriage and re-balancing China

Beka Kiria (@bekakiria)



Historically, the first stage of global order transformation took place after the first World War, which had a temporal soothing effect. Perhaps the most damages encountered by a number of great economic powers. Furthermore, an intricate system of alliances induced imperial and colonial rivalry for wealth and resulted in an fiasco for the European balance of power.

The second wave of shift of the global paradigm occurred after the second World War. International actors claimed neighboring territories and the expansionism was the driving force of nationalistic states for expanding territorial boundaries by means of military aggression.

At the end of the second World War, the U.S. perceived and ranked the involvement in the European Security framework as the top national priority in order to avoid the emergence of a new hegemonic power in Europe. Thus, two world wars completely wiped out the previous European balance of power. The risk that the Soviet Union could succeed where Nazi Germany had collapsed inevitably elicited the U.S.-European security partnership.

Subsequently, during the Cold War bloc based security systems emerged and European states along with the U.S. established a number of security institutions. The Main aim of multi-layered institutional arrangements was to prevent and avoid the Soviet pressure and influence on the rest of Europe.

After the collapse of the Soviet Union, the U.S. enjoyed the role of the only remaining superpower. After a while though, China has emerged while the Russian Federation came back to the political stage and the world turned toward the multipolar order.

Earlier, hegemonic dominance of the U.S. successfully fostered the NATO enlargement process. Starting with the German reunification, the Visegrad Group, the Vilnius Group and finally reaching aspiring countries like Georgia and Macedonia. However, due to the geographical location NATO faced challenges and difficulties from a newly emerged Russian Federation.

In spite of intensive cooperative frameworks with particular stakeholders in targeted countries and regions, a possible NATO membership of Georgia and Ukraine became a difficult task due to Russian aggression with a strong opposition to any NATO extension plans.

On top of that, the long-term strategic shift by the U.S. from Europe to Asia puts the Euro-Atlantic security cooperation into question. There is no clear projection, whether the U.S. security planners will focus on the Asian continent and let Europe face challenges alone or transatlantic relationship will remain steady. [In my opinion, the development of US troop contributions and deployments on the European continent since 2014 have kind of answered this question.]

Moreover, the EU is enthusiastic about developing a European military dimension which could undermine NATO [My personal opinion: I don't think so. European integration will not weaken but strengthen interoperability within NATO. "Either or" is too easy in this respect.]. However,

the Russian activities in Ukraine are jeopardizing the concept of a Europe whole, secure and free, resulting in an U.S. roll back of its rebalancing strategy. In a chain of political reactions, Russia unconsciously acts as a Great Wall to hinder the U.S.' re-balancing strategy against China.

Nevertheless, China feels comfortable as long as the Russian Federation acts as a Great Wall.

Accordingly, the western position in this game must re-focus on a practical cooperation and extended a dialogue on the Central Asian region. Hence, there is almost non-existent institutional outreach of NATO and EU. Therefore, geographically Central Asia is divided between Russia and China.

Therefore, Central Asian countries due to their geographic location are left with the choice of alliances. In comparison to Eastern European countries, Central Asian countries are facing only two emerging pathways with a vague future: developing China and the Russian Federation.

Thus, a key of success is to look through the prism of China on the Central Asian region. Not mentioning the fact that, these territories in the past were under Chinese imperial influence. Still, recent developments illustrate that China's current bid on its own Central Asian provinces - Xinjiang and Tibet greatly effects Central Asian states. [What developments? Please be more clear here.]

In this regard, the outreach of EU institutions is very weak in this region. Thus, EU presence here is understood through the chain of "neighbors of EU neighborhood". Besides, comparing the EU's presence to China, Central Asian countries are immediate neighbors for Beijing. By contrast, referring to the Russian approach towards Central Asian countries, still these states are claimed as the sphere of influence similarly as the Caucasus is claimed as Russia's backyard.

In advance, a common shared value in the 21st century in scope of the transatlantic relationship is not important anymore. [What do you mean by that? What common shared value do you mean?] Emerging powers, such as China, Brazil and India are far more attractive for U.S. interests. As outlined above, the strategic move from Europe to Asia temporarily sacked the U.S. strategic maneuver.

Finally, from the wider global context, the strategic move from Europe to Asia is a critical necessity. Meanwhile however, the U.S. must keep the strong Euro-Atlantic bond, avoid the realization of the EU's military dimension and protect the concept of a Europe whole, secure and free in order to remain the sole superpower.

Beka Kiria worked at the Ministry of Defence of Georgia in capacity of Senior Specialist at Defence Policy and Planning Department. He practically engaged in development of national defence and security documents. He focused on legislative review in defence and security sector, including the composition of written suggestions before the law bills formally intruduced to the parliament. Beka become a New Security Leader at Warsaw Security Forum 2015. Beka publish articles at the world leading magazines, such as The National Interest, European Defence and Security magazine. He graduated from the University of Leicester UK, earning degree in Public International Law. Earlier, before studied International Relations at Cambridge Art and Science College, UK.

Innovation Breakthrough: Augmenting NATO's Role in Collaborative Defense R&D

Miklos Bodnar (@MikBodnar)

Since the end of the Cold War, numerous obituaries have been written for both the NATO alliance and the need for collaborative security in our modern times. Whether it be the lack of apparent threats or a mentality that unilateralism trumps collaboration, many believe that nations are best positioned to achieve their national security goals on their own. However, both the security environment of the past 25 years and the resources available to NATO allies in that timeframe acutely expose the fallacies of such a mindset. As security risks have become more complex and global and the Global Recession has strained defense budgets, NATO allies no longer can rely on a single nation or even a few strong members to address these challenges. Correctly, NATO identified the difficulties arising from strained defense budgets and promoted its Smart Defense policy in 2011. To further execute the goals of this policy, NATO should not only leverage its advantages in current force structure and economic output, but the underlying technological prowess in each nation's industrial and academic base. The Alliance can nurture a community of knowledge to better identify R&D resources within member and partner nations. For NATO to become a focal point for collective defense research and development (R&D), it will need to add tools to existing science and technology (S&T) components, create a new agency tasked with a unique high risk, high reward R&D role, and integrate non-Member partner nations to ensure access to the best science.

Currently, NATO's Science and Technology Organization (STO) is tasked with leading the S&T efforts of NATO, primarily through the Collaboration Support Office (CSO). STO-CSO has been very successful at providing a forum for allied nations, partner industries and military labs to conduct peer-reviews and technical assessments for ongoing research. However, while this augments awareness of similar research in a range of technical fields, more can be done. STO-CSO should create and manage a database of ongoing research programs applicable to reinforcing NATO military capabilities (e.g. sensors, autonomy, cyber/big data, warfighter performance, etc.). This database will consist of nation contributions of program information, particularly ongoing programs in national defense laboratories. Additionally, the database will provide a Solicitation Marketplace where allied and partner nations can post future research projects in need of industry and academic proposals for potential research performance. In order to ensure fair and open solicitation for both industrial (major defense and small-medium enterprises) and academic organizations that are not experienced with working on defense research projects, STO-CSO will create a set of guidelines regarding performance of research. These guidelines will include rules and regulations on contracting, budgeting, intellectual property rights, export control, and security protections.

If NATO is serious about being an ambitious centerpiece to allied security, then it must take on part of the burden sharing necessary with regards to defense R&D. NATO STO could establish a project management agency to fund and manage high risk R&D projects that are too challenging for individual nations. The agency would recruit scientists and engineers with revolutionary,

innovative concepts for a limited duration, during which they would manage a budget and program hoping to achieve breakthroughs for said concepts. Research performance would be conducted by government/defense labs, industry, and academia, utilizing a similar open source selection process that is currently used by the NATO Security Investment Programme (NSIP). All nations would contribute to the agency's overall budget, but research budget allocation would be based purely on scientific benchmarks, not national contribution levels. Upon completion, the agency would work with STO-CSO for technical transition to interested nations or even the commercial sector for further maturation.

Far too often, revolutionary scientific concepts and ideas fail to recruit the political and monetary support needed given the high probability of failure. This deterrent is especially true for nations and industries where resources are limited and the ability to take on risk is inherently difficult. Additionally, the best science does not always choose NATO allies. The NATO Science for Peace and Security (SPS) Programme currently attempts to address the promotion of science cooperation between NATO and non-NATO partners. SPS can be a framework for the integration of partner nations into both the STO-CSO database/marketplace and the high risk R&D program management agency. Involved partner nations would have access to conduct R&D work, but would not be involved in the program management and decision making processes on NATO driven projects. This would allow for NATO allies to ensure the R&D would coalesce with Allied goals, while still ensuring access to R&D resources outside member nations. Once a partner nation's lab, industry, university performs work under NATO funded R&D, they are treated the same as an organization from a member nation. This collaboration with partners will create stronger relationships between S&T organizations and increase access to innovative R&D.

While NATO remains a valuable forum for political-military discourse, its primary mission must remain preparing and providing the military capabilities needed for the security of member nations. The advanced science and technology base in Europe and North America are a competitive advantage that other nations or groups do not possess. But identifying and matching the research and development to the security application and need is difficult. There also exists a bureaucratic resistance to risk and potential failure that permeates scientific discovery. With a new approach to collaborative defense R&D, NATO is in a unique position to take on these challenges and foster the investments that will propel the Alliance's future capabilities.

Policy Recommendations

1. NATO STO-CSO S&T Tools
    a. Creation of database for all ongoing in-nation defense R&D research programs
    b. Creation of R&D project "Marketplace" to solicit proposals from industry and academia
    c. Formalize guidelines for defense R&D contracting
2. Stand up a program management agency to fund high risk R&D
3. Integrate partner nations into S&T tools and agency to increase R&D innovation access

Mik Bodnar has had a key interest in Trans-Atlantic defense issues throughout his career. After graduating from Syracuse University with an M.A. in International Affairs, he completed an

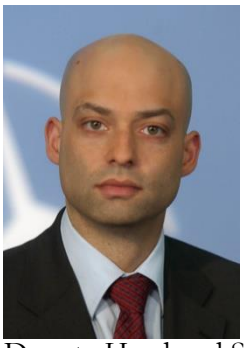
internship with NATO Operations Division, gaining valuable insight on the daily military missions of the Alliance. Since 2011, he has worked at the Defense Advanced Research Projects Agency (DARPA), a research and development wing for the US. Department of Defense. As an International Cooperation Specialist, he provides advice and administration for defense scientists on collaborative R&D opportunities with partner nations. Mik is originally from Los Angeles and plays recreational softball every spring.

Dinner Dialogue:
Germany & NATO – Leading from the Center?

Mr. **Eric Povel** is the Program Officer in the Engagements Section of Public Diplomacy Division (PDD), NATO since October 2012, dealing with Afghanistan and NATO's other Operations. He also holds country responsibility for Belgium, Germany and the Netherlands. From 1989 until 1995, he worked for a number of public affairs consultancies in The Hague. As of May 1995, Mr. Povel works in NATO's international staff, firstly, at the Netherlands Information Officer in the PDD at NATO Headquarters in Brussels. After NATO's Kosovo air campaign in 1999, Mr. Povel became the media planner for NATO's yearly Crisis Management Exercise (CMX). In July 2011, Eric Povel was the Strategic Communications Coordinator, heading the PDD StratCom Cell in support of the Assistant Secretary General for Public Diplomacy, responsiblefor all operational and doctrinal StratCom issues at NATO HQ.

Christoph Schwarz

Early Bird Breakfast



James Appathurai is the NATO Deputy Assistant Secretary General for Political Affairs and Security Policy and the NATO Secretary General's Special Representative for the Caucasus and Central Asia. He holds degrees in Political Science and History from the University of Toronto and in International Relations from the University of Amsterdam. After starting his career as editorial assistant in the Canadian Broadcasting Corporation in Toronto in 1993, he worked as Policy Officer in the Canadian Defence Department in Ottawa. From 1998 to 2004, Appathurai joined NATO as Deputy Head and Senior Planning Officer in the Policy Planning and Speechwriting Section of the Political Affairs Division. Before being appointed Deputy Assistant General Secretary of NATO and Special Representative for the Caucasus in 2010, he had served as NATO's Spokesperson since 2004.

Bundesakademie für Sicherheitspolitik

British Embassy Berlin

Deutsche Atlantische Gesellschaft e.V.

NATO TALK
around the BRANDENBURGER TOR
BERLIN

YATA Germany

Agenda

NATO 4.0 – A NEW NATO FOR NEW CHALLENGES?

Venue: Press and Information Office of the Federal Government,
Reichstagufer 14, 10117 Berlin

Saturday, November 12

1:00 p.m.	Welcoming Coffee and Opening Remarks
1:30 p.m.	Joint Walk to the Pier
2:00 p.m.	Politics on Water – Berlin Boat Tour
3:30 p.m. - 6:30 p.m.	Working Group Session
7:00 p.m.	Joint Dinner, Kartoffelkeller, Albrechtstraße 14B, 10117 Berlin

Sunday, November 13

9:00 a.m. How to deter digital warriors? NATO and the cyberspace

The issue of security in the cyber space is of ever increasing importance – underlined by NATO's recent decision to define cyberspace as a war-fighting domain and the joint assessment that 'interconnectedness means that we are only as strong as our weakest link.' How can the Alliance make sure that strong and resilient cyber defenses enable it to fulfill its core tasks – especially with regard to collective deterrence or even defense? Which political, strategic and technical issues need to be addressed so that NATO can really become 'cyber aware, cyber trained, cyber secure and cyber-enabled' in the near future? In turn, with the difference between defensive and offensive digital warfare being marginal, how can such conflicts be managed and potentially de-escalated?

Introduction and Moderation:
Mattia Nelles, Free University Berlin & Alexander Schroeder, German Armed Forces

Speakers:
Isabel Skierka, Researcher, Digital Society Institute at the European School for Management and Technology (ESMT) in Berlin

NATO OTAN

This event is co-sponsored by the North Atlantic Treaty Organization

Sebastian Mueller, Desk Office Cyber Security, Federal Foreign Office

Dr. Olaf Theiler, Section Head Future Analysis at the Bundeswehr Planning Office

10:30 a.m. Coffee Break

10:45 a.m. In for the long run? NATO's future role in crisis management

Preventing and managing crises, stabilizing post-conflict situations and supporting reconstruction – how attainable are these goals for NATO and how can existing strategies and instruments be improved? Crisis management operations have played a crucial part in NATO's post-Cold War transformation. But to what extent can peace-keeping missions like KFOR in the Balkans and RSM in Afghanistan be expected to also be a part of NATO's adjustment to the current "Article 5-World"? If so, what are the lessons that can be drawn from past operations and to what extent can they be rendered useful for future missions in a context of "intervention fatigue" on the one hand and an unraveling security environment on the other?

Introduction and Moderation:
Magdalena Kirchner, RAND Corporation & Chris Zrenner, University of Passau

Speakers:
GenLt. Frank Leidenberger, Commander German Multinational Corps Shares / Basic Military Organization, German Army Command

Mihai Carp, Deputy Head of Section in the Operations Division of the International Staff at NATO HQ

Nicole Birtsch, Research Associate, German Institute for International and Security Affairs

12:15 a.m. Lunch, Restaurant "Die Eins", Wilhelmstraße 67A, 10117 Berlin

1:30 p.m. Enlargement, enablement, entrapment? NATO's future approach to cooperative security

When policy makers and experts address the numerous challenges NATO faces today outside of its members' territory, security partnerships and defense capacity building are core instruments to prevent resource-intense and domestically contested out-of-area operations. Yet, they allow the alliance's members to further maintain or even enhance their influence on peripheral states, containing therefore transnational security risks and destabilization. In times, where NATO's Open Door policy seems to have reached its limits, has enablement become the new enlargement? What does this mean for new members of the alliance such

as Montenegro or traditional pillars of cooperative security such as Israel? Can mutual expectations be harmonized or is a „two-class"-system of security inevitable?

Introduction and Moderation:
Sebastian Feyock, German Council on Foreign Relations

Shalva Dzidziguri, Research Fellow, Georgian Center for Security and Development

James Mackey, Head of Euro-Atlantic and Global Partnership, NATO

Capt. (N) Arvi Tavaila, Defence Attaché, Finnish Embassy Berlin

3:15 p.m. Coffee Break

3:30 p.m. Working Group Discussion

6:00 p.m. Presentation of the Recommendations/ Wrap-Up

7:30 p.m. Conference Dinner: Germany & NATO – Leading from the Center?
Introduction and Moderation:
Mattia Nelles, YATA Germany

Eric Povel, Program Officer in the Engagements Section of Public Diplomacy Division, NATO

Christoph Schwarz, Senior analyst, White Paper Project Group, German Ministry of Defense

Restaurant: Oranium Corner, Oranienburger Str. 33, 10117 Berlin

Monday, November 14

7:45 a.m.	Early Bird Breakfast Distinguished Guest: Mr. James Appathurai, NATO Deputy Assistant Secretary General for Political Affairs and Security Policy & Special Representative for the Caucasus and Central Asia Café LebensArt, Unter den Linden 69A, 10117 Berlin
9:00 a.m.	Main Conference "NATO 4.0 – A new NATO for new Challenges?" Hotel Adlon Kempinski, Unter den Linden 77, 10117 Berlin
6:45 p.m.	Concluding Remarks / Reception at the Embassy of the United Kingdom in Berlin

This event is co-sponsored by the North Atlantic Treaty Organization

Bundesakademie für Sicherheitspolitik

Presse- und Informationsamt der Bundesregierung