

ATLANTIC TREATY ASSOCIATION

Volume 2 - Issue 9, September 2012

Playing a direct role in Estonian civil society, the Estonian Atlantic Treaty Association (EATA) has taken the initiative to address the problems of division within the Estonian education system. In an effort to increase dialogue and cooperation between the Estonian and Russian communities living in Estonia, the EATA established regular seminars in schools across the country to bring this new approach to both Russians and Estonians alike. By engaging teachers and students from both communities, the EATA has created a new interface that has already begun to help foster a better mutual understanding and ease historic tensions throughout the population.

As one of the most pressing national security issues of the 21st century, the threat posed to critical infrastructure by a cyber attack has taken an alarming toll on analysts and policy-makers throughout the world. With a more interconnected world at our fingertips, the challenges posed to a state's critical infrastructure has never been higher since threats can materialize abroad, be launched within seconds and wreck devastation across a country while hiding the identity of the attacker. By analyzing the threat level and current state of policy, analysis shows which gaps must be bridged and where cooperation is necessary in order to safeguard critical infrastructure from its current state of immense vulnerability. -

Jason Wiseman

CONTENTS

Global Pulse: Sanctions Are Emboldening the Iranian Regime

Mahsa Alimardani analyses the toll that international sanctions are taking on the Iranian population and argues that the nuclear program distracts the West from their core objectives while permitting the regime to continue with its on going human rights atrocities.

RUSSIAN-ESTONIAN RELATIONS IN EDUCATION



The Estonian Atlantic Treaty Association examines the faults of the current education system in the Baltic's and sheds light on the measures the EATA has taken to foster a new educational atmosphere to help create better relations between Estonians and Rus-

sians.

CYBER SECURITY AND CRITICAL INFRASTRUCTURE

Lior Tabansky analyzes the danger posed to critical infrastructure by cyber threats and how the current lack of sufficient international cooperation has left states particularly vulnerable. Lior analyzes the key issues for policy makers on the national and international levels

and argues that greater collaboration and integration between states is the key to formulating effective policy that can protect critical infrastructure around the world.





GLOBAL PULSE

Sanctions Are Emboldening the Iranian Regime

By Mahsa Alimardani

The sanctions noose around Iran fully tightened at the beginning of July as the European Union joined the United States to impose a total embargo on all purchases of Iranian oil and place severe restrictions on the country's central bank. These sanctions have resulted in harsh realities for ordinary Iranians. The price of chicken has reached an unprecedented high, tripling from 22,000 to 66,000 Rials in just the last two months. The nation's consumer price index has risen 22%, and its oil revenues have dropped by almost 50%. Unemployment, particularly among youth, is rampant.

The aim of Western sanctions is to coerce the Iranian regime to comply with international rules over its nuclear program. What the Europeans, the US, and Israel ultimately hope to achieve is a powder keg of discontent between the Iranian people and the regime that could go off at any moment, empowering Iranian society to topple the regime.

There have also been increasing drumbeats for war these past few months, echoing out of Israel, and among more conservative American politicians. For now however, President Barak Obama remains hesitant to tackle the military option two months before the presidential elections. The Obama

administration's current policy is to allow the new sanctions more time to produce an effect.

But how much longer should the people of Iran wait? Iranian people have been under the direct effects of sanctions since 1995, when the oil and gas sector was first targeted, to the pre-

sent day where banking and financial sectors have left private enterprise and ordinary citizens as the primary and overwhelming victims. Imposing what US Secretary of State Hilary Clinton has termed

"crippling sanc-

tions" renders the well being, human rights, and reform aspirations amongst the Iranian people trivial.

Payam Akhavan, a human rights lawyer and founder of Iran Human Rights Documentation Centre, says "[Western politicians] only care about nuclear energy and Iranian oil. In fact,

Iranian human rights issues are at the bottom of their list."

As the likelihood of war increases it is important to ensure that the nuclear issue does not overshadow human rights concerns.

It is too often easy to demonize the regime for its draconian rule, while forgetting the struggles of individual Iranian lives. Although the West expects Iranians to turn against their regime



Iranian citizens are cashing out more and more Rials for basic goods like poultry, milk and bread (Photo: BBC)

The Obama administration's current policy is to allow the new sanctions more time to produce an effect.

because of the debilitating effects of economic sanctions, it is particularly difficult for Iranians to side with the West due to the vivid memory of the Iran-Iraq war and the West's ambivalence towards Saddam Hussein's use of chemical weapons against Iranian troops.

Sanctions are not only a reflection of Western hypocrisy, they further serve to embolden the very factors that make Iran an undemocratic state. While ordinary Iranians struggle to afford their milk, chicken and bread, Iran's Revolutionary Guards Corps (IRGC) (formed in 1979 to preserve the values of the Islamic Revolution) continues to thrive. IRGC guardsmen control most relevant ministries within Iran, including the Ministry of Petroleum. The IRGC's economic wing, which controls roughly 50% of the nation's economy, is notorious for operating like a private mafia. The current economic isolationism that the West is subjecting Iran to is aiding their operations.

As most Iranians struggle to feed their families through legitimate means, those inclined towards more nefarious sources can turn to the black market that is directly supplied and controlled by the IRGC. The Guard engages in large-scale smuggling of not only illegal products such as alcohol and opium, but ordinary goods that they import without tariffs or inspection. This economic clout further strengthens the IRGC's rigid military structure, including the paramilitary Basij. The hopes of a civil society uprising in view of economic discontent will only be met by the brute force of these ruthless military arms. This was of course best exemplified by the Basij's bloody crackdown on protesters in 2009.



Sanctions prove ineffective when faced with the all powerful IRGC which controls the economy, military, and black market (Photo: Iran Focus)

As one Iranian women's rights activist has stated, "The international community's sole focus on the nuclear issue has resulted in the adoption of policies that inflict great damage on the Iranian people, civil society and women. Militarization of the environment will prompt repressive state policies and the possibility of promoting reform in Iran will diminish."

Since sanctions are seemingly preserving the oligarchic Islamic regime, we have to ask what can we do for Iran, short of attacking the country. (The problems of a military strike being the subject of another op-ed).

I suggest it lies in forming a relationship with Iran based on human rights. We must recognize that the biggest threat to the Iranian regime will not come from

the West, but from the Iranian people. We must look to their individual struggles and see how we can properly sanction the individuals responsible for diminishing their freedoms, not embolden them.

It is time to redirect our focus towards the implications of solely focusing on the nuclear policy of the Iranian regime. When the nuclear capabilities of Iran become the sole concern of the international community, it becomes easy to forget the murderous bureaucracy that remains in place. It is easy to presume that if Iran were to abide by international standards for its nuclear program that the West would easily forget the other egregious issues facing the Iranian state.

After all, these sanctions are not holding into account the actions of Iranian Justice Minister Esmail Shooshtari, or Interior Minister Mostafa Pourmohamadi who commissioned the deaths of more than 15,000 political prisoners in the 1980s. A culture of impunity reigns within the Iranian regime, and sanctions against the country's nuclear program only work to further intensify this.

Mahsa Alimardani is a recent University of Toronto graduate and guest contributor at the Atlantic Council of Canada. She's been a reporter for Taiwan's Taipei Times, as well as a writer for the Huffington Post. She wrote her senior honours thesis on the women's movement in Iran, and is taking a year off to write and travel before returning to academia at University College of London for a Masters in Human Rights.

Approaching Russian-Estonian Relations for the New Generation

by Estonian Atlantic Treaty Association

A situation familiar to many post-soviet countries, Estonia is facing several crossroads in its education policy. First, is the question of language – should we or can we make Russian students learn Estonian subject matter in the Estonian language? Second, how should some of the more disputable issues relating to Estonia's past be taught? The Estonian Atlantic Treaty Association (EATA) has dealt with this matter in the form of civic activism for seven years.

As one can imagine there are several painful episodes in Estonia's history which touch us more closely than the rest of Europe even though Europe itself has not reached finalizing agreements on these issues. If countries are still disagreeing on the causes and outcomes of World War II, debating over whether or not to use the term "occupation", "annexation" or to come up with something softer, how should we teach these matters to young children in our schools?

Estonia's population is made up of about 30% of ethnic Russians among whom the knowledge of Estonian language varies greatly. Moreover, the concepts people have of historical events and the roles played by different countries varies widely. The Estonian society is gradually modernizing in its attitudes as different communities are becoming more accepting of one another. However, the traditional education system still needs to teach facts. History teachers need to provide dates, name names and give reasons behind events. And children are graded on how well they learn these facts.



Estonian President Toomas Hendrik Iivess Addresses the United Nations (Photo: UN)

Fact-Centered Education No Longer Adequate

This classical fact-based education system is also one of the reasons why certain narratives are so deeply rooted in Estonian society and why it has become so difficult to eradicate them. Let us take for example the aforementioned debate over whether Estonia being made part of the Soviet Union was a voluntary decision or a forceful occupation. As one can imagine Estonians have their own opinion on the matter while the Russian community living in Estonia has a slightly different view. All this has been debated over and over again for many years and the aim of this article is not to establish historical facts but to shed light on how the EATA is working towards building a common understanding of Estonia's identity as an independent sovereign country in the past as well the present.

Estonian schools teach all subjects (including history and social sciences) based on a national curriculum issued by the Estonian Ministry of Education and Research and use the same textbooks. However there are several variables which influence the outcomes in Estonian schools and in Russian-language schools in Estonia. First, teachers in Russian-language schools have traditionally received their higher education in the universities of Moscow and St Petersburg during the soviet and post-soviet eras. Second, for a myriad of reasons, the Russian-speaking population in Estonia mainly follows the Moscow-minded media from Russia. At several points in Estonia's history, the national curriculum of history clashes with how teachers have been educated in Russian universities and what the media presents as being accurate. As I am sure you can imagine, the aforementioned factors are more influential to a young student in a high school classroom than the facts and figures presented in the curriculum which are written in a relatively complicated, textbook-style Estonian language.

Methods of Approach

In 2006, the EATA set out on a mission to try and reach teachers of history in Russian speaking schools in Estonia with the intent of introducing a new approach of mutual understanding and teaching based on ideas and concepts, not solely on facts. To that end, the EATA started organizing two and three day seminars for teachers from Estonian and Russian-language

schools, to bring them together and broaden their horizons in matters relating to history, security, defense policy and international relations. All of which are directly linked to the history and social sciences these teachers teach. The broader aim of these seminars is to reach the generation of young Russians living in Estonia to help shape their understanding of how a free and independent Estonia is a valuable place to live for all people regardless of their ethnic origin.

Without a doubt, this method of carrying out seminars is not coincidental. EATA seminars always last two to three days in order to help create an environment where teachers of Estonian schools as well as Russian-language schools have the opportunity to freely mingle and carry conversations in an informal atmosphere so they can get to know each other's views better. Another very important factor in the EATA's approach to getting teachers to open up to new ideas is lining up an array of ministers, diplomats, high governmental officials and well-known experts on defense policy – people whose names and images are respected and appreciated both among the Estonian and Russian communities living in Estonia.

Establishing direct contact between history teachers and high-level experts in the field has created a strong appreciation amongst both parties, leading to a greater and more valued role for the EATA's seminars. Opinions expressed and statements made under Chatham House rules offer an invaluable insight to the inner workings of Estonian society and governmental institutions that are often hidden by those who do not have direct contact with these institutions. These pieces of information, although not quotable, contribute immensely to broadening teachers' horizons in the topical matters of defense and security policy and international relations.

Bringing together teachers from both the Estonian community and the Russian community in Estonia has been more effective than just concentrating on the teachers of Russian schools. In order to integrate the two cultures living in Estonia, it is essential that both conform and adjust to the new realities of modern Estonia while not disregarding its past.

In order to integrate the two cultures living in Estonia, it is essential that both conform and adjust to the new realities of modern Estonia while not disregarding its past.



19th Summer School of the Estonian History Civics Teachers' Association (Photo: European Association of History Educators)

Integration From Both Sides

One of the essential goals the EATA is working towards achieving is rooting a deep understanding among Estonians that the term "Russian" does not equate "communist" and the wrongdoings of totalitarian regimes are not to be considered visceral to the whole Russian nation. Therefore gathering together a group of nearly a hundred teachers, half of whom are Estonians, half are Russians, and providing them with the exact same lectures, trainings and workshops, is a highly effective way of communicating the message of shared common values that form the foundation of a state.

On average, a teacher in the schools of Estonia has direct contact with approximately 100 children, therefore 80-100

teachers participating in EATA's seminars help make a significant difference in how Estonia's young generation perceives the notions of independence, sovereignty, good governance and democracy.

Since it is always immeasurably more difficult to break the stereotypes and fossilized concepts amongst the older generation, it is the young people studying in Estonia's middle schools and high schools that are open to new perceptions and whose attitudes are not yet fully conformed. By contributing to raising a young generation that can critically evaluate the information presented in the media, text books and by their history teachers, we are helping make sure that the Estonia of a restored independence, itself in its early twenties, develops into a mature, tolerant and multicultural society and that its citizenship is valued by its inhabitants and its independence is respected by everyone living in Estonia.

The views expressed in this article are entirely those of the author. They do not necessarily represent the views of the Atlantic Treaty Association, its members, affiliates or staff.

By Lior Tabansky

International Cooperation in Critical Infrastructure Protection Against Cyber Threats

A functioning modern society depends on a complex tapestry of infrastructures: energy, communications, transportation, food, and many others. The cyber threat to critical infrastructure is perhaps the most significant issue in the realm of cyber security. In today's reality, the existing computerized infrastructure can be exploited through penetration of communications networks or the software or hardware of the command and control computers in order to disrupt, paralyze or even physically destroy a critical system. This threat stems from the unique vulnerability inherent in the properties of cyber-space and is thus fundamentally different from the traditional threats.

The "Stuxnet" affair is the best known event proving the gravity and the uniqueness of this new threat. The Stuxnet worm virus began by infecting Windows-based computers. Among those, it searched for computers running Siemens-produced industrial command and control software of a certain type connected to an industrial controller of a specific model. Only if the computers met all these conditions, would the virus then go on to activate another software code that disrupted the activity of the computerized controller, while concealing the change from the control software and equipment operators. This way, Stuxnet allegedly damaged the proper operation of the centrifuges for uranium enrichment in Iran. Despite various speculations, the source and duration of the attack cannot be known from analyzing the weapon itself.

Critical (information) infrastructure protection (CIP) is a developing new field of national policy in cyber-security.

Although at first glance, it appears that CIP belongs to the

realm of computer engineering, upon further examination it becomes clear that it should be expanded beyond the technical aspect. Indeed, the major challenge in protecting critical infrastructures from cyber-threats is not a technical, but a strategic and political



Soldiers Monitoring Cyber Security (Photo: FrumForum)

issue. Today, most states have legal and technical regulations for selected sectors. However, policy and regulations on a national level are insufficient to tackle the global nature of cyber-security.

A Novel Threat

Infrastructure is defined as critical when it is believed that

disrupting its function would lead to a significant socio-economic crisis with the potential to undermine the stability of a society and thereby cause political, strategic, and security consequences.

Recent years have brought about in-

creased concerns over the potential vulnerability of the infrastructures that are the basis of developed modern societies, yet the fact that this discussion is taking place now is surprising, given the strength of defense in the developed world.

The importance of critical infrastructures is obvious and that is why they have always been lucrative targets. In 1917, during the Bolshevik Revolution, Lenin and Trotsky ordered their forces to take over the post office, telegraph systems,

The major challenge in protecting critical infrastructures from cyber-threats is not a technical, but a strategic and political issue.

bridges, and train stations. In World War II, huge efforts have been made to hit critical infrastructures in order to degrade the enemy's fighting ability and spirit. Throughout history states have erected defense systems for their infrastructures: camouflage, guarding, fortification, defensive forces, deterrence, etc. Why then, is there a growing concern about damages to critical infrastructures, particularly in the strongly developed countries enjoying peace through military superiority over their respective enemies?

Practically, all of the traditional infrastructures have gradually become information infrastructures since they incorporate computerized devices. In addition, new purely informational critical infrastructures have been created: databases storing important computerized data, such as records of capital in the banking system, scientific and technical intellectual property, and the programmed logic that manages production processes and various business dealings.

These include mainly data communication systems and computerized methods of automatic command and control, which improve efficiency but also create new vulnerabilities. The major challenges stemming from the characteristics of cyber-space as it exists today are:

- the wide-spread use of off-the-shelf commercial technologies,
- the difficulties distinguishing a glitch from an attack,
- establishing a causal link between an event and a result,
- tracing the source of the damage, and
- identifying the attacker, even if the geographical location is known.

These properties of current cyber-space create an unprecedented vulnerability in critical infrastructure. For the first time in history, it is possible to attack strategic targets (such as critical infrastructures) via cyber-space - without physically reaching the location, without confronting defensive forces, without exposing the attacker's identity, and even without an exposure of the attack itself.

Issues for Policy-Makers

Confronting the threat to critical infrastructures includes prevention, deterrence, identification and discovery of the attack, response, crisis management, damage control, and a return to full capability. The problem is perceived as a technical one, and therefore, the proposed solution is an engineering solution. This "information security" is often over-emphasized. Any discussion on protection and defense measures begins with prioritization. Here, a precise engineering formula for dealing with the cyber threat is not possible: the society's structure, values, and institutions are integral parts of the environment, affecting the problems and the feasibility of various solutions. On the national strategic level, CIP actually becomes a protection of our information-based society. Information security is a necessary but insufficient technical part of the strategic vision. A comprehensive national policy on CIP must take into account the complex social,

political, economic, and organizational aspects. Representative political institutions are in place for such a process in a democratic society. Given the constraints of the political system, such a discussion will presumably be lengthy and at times frustrating. Nevertheless,

only through a joint political process will it be possible to design an optimal response to the threat for the long term.

National-Level Policy

Two examples of contrasting national cyber-security and CIP policies presented henceforth stress the political and cultural aspects of cyber-security policy. Open societies shy away from state intervention in business processes. Thus, the arguments against government regulation of the internet originate from the "free market" ideology. Since the mid-1990s, the critical infrastructure protection policy in the United States was based on market mechanisms, industry standards and voluntary "private-public partnership". Recently, there are calls for giving broader powers to the government to guide and supervise cyber-security aspects.

Israel has implemented a different, more centralist policy. Israel is the only developed country that is under ongoing military threat that is manifested in a variety of ways: SCUD

Only through a joint political process will it be possible to design an optimal response to the threat for the long term.

ballistic missile attacks in 1991, frequent terrorist acts, suicide bombers in 2000-2005, and ongoing rockets shelling in the north and south of the country. Israelis thus value "free market" less than their national security. Since 2003, a national CIP policy has been implemented in Israel. The state of Israel established a designated body - the National Information Security Authority (NISA) - for oversight and guidance of critical infrastructures, both private and state-owned. The point that strikes our American counterparts is that while the company is obliged to follow government instructions, the company alone bears the entire costs for protection. This arrangement has been working for years, raising almost no objection. One plausible explanation of such compliance is the companies' benefit of having custom-tailored security designed by state-of-the-art specialists. The Israeli government has further expanded the scope of this state intervention in its market economy since the summer of 2011.

Any other national policy is also affected by a wide range of values, constraints and interests. But despite the importance of the national policy, international cooperation is nothing less than crucial for cyber-security.

The Supra-National Level: NATO and EU as Enablers of Cooperation on Cyber-Security

The trans-national character of the telecommunications network and the internet is widely acknowledged. Any discussion on cyber-security stresses the need for international cooperation. At least 12 major international organizations address issues concerning the ICT infrastructure and cyber-security. Information and intelligence sharing, a common understanding of the threat and mutual trust are crucial for cyber-security. However, given the competitive anarchic structure of the international system as described by the Realist theory of International Relations, such deep international cooperation is extremely unlikely. This begs an important question, is the future of cyber security and CIP doomed to isolated, national endeavors?

On the international level, cooperation is only likely to occur via alliances of like-minded states. This is where the significance of existing cooperative arrangements comes into play. Without delving into the legal and formal definitions, both NATO and the EU are voluntary cooperations between like-minded states. Common cyber-threats and CIP needs should provide further ground for a continuous cooperation.

NATO has acknowledged this and is promoting co-operative action in several directions. The recent Lisbon "Strategic Concept" has stressed the urge for an immediate international cooperation of the member states in order to develop and coordinate the national cyber defense capabilities under a centralized command for a better protection. The NATO Group of Experts report recognized the increased reliance on information systems and recommends the Alliance to "contribute to the broader security of the entire Euro-Atlantic region." The revised NATO Policy on Cyber Defense, adopted in June 2011, outlines NATO's efforts in cyber-defense throughout the Alliance and

also establishes the principles for NATO's cooperation with partner countries, international organizations, the private sector, and academia. The Cyber Defense Management Authority in Brussels works on standards by which NATO could determine its responsibility to assist member states in a case of emergency. The Multinational Cyber Defense Capability Development (MNCD2) program intends to facilitate cyber-defense through collaboration.

The Council of Europe Convention on Cybercrime states that "security and the protection of rights is the responsibility of both public authorities and private sector organizations". A European Programme for Critical Infrastructure Protection (EPCIP), aimed at both European and national infrastructure, has been initiated by the European Commission. The European Commission's Programme Framework-7 (FP-7) has allocated 1.4 billion Euros for security innovation research. The European Network and Information Security Agency (ENISA) is "a body of



IDF Field Commanders Learn About Cyber Warfare (Photo: Jerusalem Post)

expertise, set up by the EU to carry out very specific technical, scientific tasks in the field of Information Security".

There are already several international initiatives on cyber-security both in NATO and the EU; this article does not survey them or evaluate their effect. An international cooperation between numerous organizations below the representative government level is a complicated task. Regardless of the success of specific NATO or EU initiatives, the fact that like-minded countries have a venue for cooperation is highly promising with regard to coping with cyber-threats. If a stable mechanism for such an endeavor evolves, it will provide an additional cyber-security capability for the member states.

Conclusion and Policy Recommendations

The central challenge in protecting critical infrastructures from the cyber-threat is not technical; it is rather a challenge of building a comprehensive national-strategic vision and determining the global character of the threat. The optimal cyber security and CIP in particular, can only be achieved through broad public discussion in a democratic political system. However, the global nature of cyber-space renders even the best possible national-level policy incomplete.

Is the future of cyber security and CIP doomed to isolated, national endeavors?

Above the national level, international cooperation will be beneficial; however, cooperation is highly unlikely in the anarchic international system of competing states. Thus, an Alliance like NATO holds an intriguing opportunity to enhance the strategic posture of its members in the information age. The EU also holds the potential to benefit its members' cyber-security by crafting information-sharing mechanisms and other cooperative measures of the existing organizational foundation.

The major recommendation is to leverage the existing frameworks of cooperation, namely the numerous vectors of contact provided by NATO and EU membership, to build trust and facilitate information-exchange, consultation and cooperation.

Another noteworthy issue is that additional formal arrangements are not necessary. Cyber-security is a domain of rapid

change and deep interconnectedness; these properties are very hard to deal with by traditional, rigid bureaucratic demarcations of organizational authority. It may even be counterproductive to introduce artificial limitations to collaboration, saying for example that NATO will only deal with military defensive topics and refrain from dealing with cyber-security that falls under other categories such as civilian CIP, crime, or intellectual property theft. Instead, an informal voluntary cooperation among peers, based on mutual interest and trust, is a sufficient and effective means of action that will both enhance national cyber-security, and further strengthen the Alliance.

From the non-member state perspective that the author of this article has, it appears that the sort of joint endeavor enabled by NATO or EU membership, will provide the member-states with an exceptionally valuable and rare layer of cyber security.

References:

James Der Derian and Jesse Finkelstein, "Critical Infrastructures and Network Pathologies: The Semiotics and Biopolitics of Heteropolarity," in Myriam Dunn Cavelty and Kristian Soby Kristensen, eds., *Securing "The Homeland": Critical Infrastructure, Risk and (In)Security* (London and New York: Routledge, 2008).

Karl Popper, *The Open Society and its Enemies* (Routledge: 2011).

Gabi Siboni, "Protecting Critical Assets and Infrastructures from Cyber Attacks," INSS, *Military and Strategic Affairs* 3, no. 1 (2011): 93-101.

Lior Tabansky, "Basic Concepts in Cyber Warfare," *Military and Strategic Affairs* 3, no. 1 (2011): 75-92.

The views expressed in this article are entirely those of the author. They do not necessarily represent the views of the Atlantic Treaty Association, its members, affiliates or staff.

About the Author

Lior Tabansky

Lior is a Ph. D. candidate at the Political Science Department at Tel Aviv University. His affiliations include the Tel Aviv Yuval Ne'eman Workshop for Science, Technology and Security and the Cyber Warfare program at the Institute for National Security Studies. He is currently writing his thesis on the Role of Advanced Technology in Israel's Struggle Against Palestinian Terrorism.

Model NATO Youth Summit Successfully Concluded in Brussels

The first annual Model NATO simulation in Europe ended on July 13th on a high note of met expectations and enthusiasm.

Coming from the North American side of the pond, where Model NATO started, I was impressed with the scale of the event in Brussels. NATO is typically involved in the organization of such simulations through providing sponsorship, organizational and expert capacity, but this is the first time that the Alliance has done it to such an extent.



The Organizing Committee of the 2012 Model NATO Youth Summit

The simulation is a very useful experience for several reasons. First, it has high educational value for those who want to understand what NATO does, how it does it and why. The issues discussed included smart defence, missile defence, cyber defence and the justifications for an intervention, among other salient contemporary topics.

A big highlight was a visit to NATO headquarters for a talk by Secretary General Anders Fogh Rasmussen about the three main tasks of NATO in the face of cooperative security, collective defence and crisis management, where he reiterated the need to uphold the values and principles of NATO to operate as a democratic, consensual organization, despite the challenges associated with doing so. Mr. Rasmussen also addressed smart defence, which is fast becoming the modus operandi for meeting NATO's commitments and operations. One important point that came out from this discussion was how the transatlantic relationship between Europe, the United States and Canada would remain firmly

in place, despite Washington's pivot towards Asia by placing China at the forefront of its foreign policy.

In the aftermath of this talk, the students were accommodated by their respective national delegations for the next several hours to discuss their position papers and national strategies. Similar to what we do in Canada, this kind of activity enriches the simulation experience immensely, because meeting the people behind major decisions really helps put into perspective how international relations are negotiated in practice, not just in classroom textbooks and slide shows.

Particularly interesting was the crisis, which involved a cyber attack against NATO on Polish radar installations. With 45 minutes on the clock to figure out what to do, the delegates very quickly managed to not only come up with a very relevant and peaceful resolution, but also had time to call in the representative of the Russian Federation for a question and answer session. This would be the sort of

*The transatlantic relationship
between Europe, the United States
and Canada would remain firmly in
place.*

performance I expect out of an experienced committee. However, only the North Atlantic Council was able to address the crisis, whereas it would typically take place across all committees of the simulation.

After having participated in both the European and Canadian model NATO's, I can say that the simulation in Europe is a much richer experience. Not just because of its closer proximity to NATO and access to key policy-makers, but because the shorter distances and better infrastructure make wider

participation possible. One feature I particularly liked, despite the mixed reactions to it, were expert panels, where for an afternoon, an expert in each issue area would visit every committee and discuss the question with the delegates to give them a better idea of how NATO would react to it.

Future simulations will create a Model NATO culture in Europe, but it will be different from the one that exists in Canada by virtue of the setting and people who organize it. Yet, it is important to encourage the communication between Ottawa and Brussels, because with a decade of experience, we are well poised to provide valuable insight into making each simulation better than the last.

A small example: a typical agenda in Canada consists of 4 questions and a crisis, and includes over a day and a half of committee sessions. The first MNATO in Europe had two questions and a crisis with more time for delegates to solve them. While this is understandable given the learning curve that must inevitably be climbed with a first-time event, it would be best to gradually increase the issue load per committee. The resulting tension would more accurately reproduce dealings inside NATO. From this point forward, the European Model NATO can only grow



MoNYS delegates at the EU Parliament for a discussion on the aftermath of NATO Chicago Summit

to become more effective, robust and better integrated. This event is a strong foundation for our future cooperation in strengthening our transatlantic links.

About the author

George Ivanov

George Ivanov is Project Manager of the Carleton University Model NATO Conference. He is an M.A. Candidate in Political Science at the Norman Paterson School of International Affairs.

ATA Upcoming Programs

On **September 14 and 15, 2012**, the Latvian Transatlantic Organization will hold its annual Riga Conference. Since the NATO summit in 2006, the Riga Conference has become a leading foreign and security policy forum in Northern Europe for world renowned political, intellectual and business leaders to gather and debate on the most acute challenges of the current international agenda.

On Wednesday **September 12, 2012**, the Belgian Association for Euro-Atlantic cooperation will host its 13th annual Euro-Atlantic Award to two M.A. students for their research thesis on NATO issues.

The Belgian Minister of Foreign Affairs, Mr. Didier Reynders and the Belgian Minister of Defense, Pieter De Crem will address the audience.

On Thursday **September 20, 2012**, at the King Edward Hotel in Toronto, Canada, H. E. Mr. Davutoglu, Foreign Minister of Turkey, will deliver a speech on Turkish Foreign policy. Minister Davutoglu will discuss the development of Turkish Foreign Policy and the challenges facing the Middle East. Reports and videos from the event will be made available on the ATA website.

Atlantic Voices is always seeking new material. If you are a young researcher, subject expert or professional and feel you have a valuable contribution to make to the debate, then please get in touch.

We are looking for papers, essays, and book reviews on issues of importance to the NATO Alliance.

Editor: Jason Wiseman

Images should not be reproduced without permission from sources listed, and remain the sole property of those sources.

Atlantic Voices is the monthly publication of the Atlantic Treaty Association. It aims to inform the debate on key issues that affect the North Atlantic Treaty Organization, its goals and its future. The work published in *Atlantic Voices* is written by young professionals and researchers.

The Atlantic Treaty Association (ATA) is an international non-governmental organization based in Brussels working to facilitate global networks and the sharing of knowledge on transatlantic cooperation and security. By convening political, diplomatic and military leaders with academics, media representatives and young professionals, the ATA promotes the values set forth in the North Atlantic Treaty: Democracy, Freedom, Liberty, Peace, Security and Rule of Law. The ATA membership extends to 37 countries from North America to the Caucasus throughout Europe. In 1996, the Youth Atlantic Treaty Association (YATA) was created to specifically include to the successor generation in our work.

Since 1954, the ATA has advanced the public's knowledge and understanding of the importance of joint efforts to transatlantic security through its international programs, such as the Central and South Eastern European Security Forum, the Ukraine Dialogue and its Educational Platform.

In 2011, the ATA adopted a new set of strategic goals that reflects the constantly evolving dynamics of international cooperation. These goals include:

- ◇ the establishment of new and competitive programs on international security issues.
- ◇ the development of research initiatives and security-related events for its members.
- ◇ the expansion of ATA's international network of experts to countries in Northern Africa and Asia.

The ATA is realizing these goals through new programs, more policy activism and greater emphasis on joint research initiatives.

These programs will also aid in the establishment of a network of international policy experts and professionals engaged in a dialogue with NATO.



ATLANTIC TREATY ASSOCIATION

ASSOCIATION DU TRAITÉ ATLANTIQUE

ATA Secretariat

Rue des Petits Carmes, 20

1000 Bruxelles

secretariat@ata-sec.org

www.ata-sec.org