THE EURO-ATLANTIC PARTNERSHIP COUNCIL (EAPC)

Established in 1997, the Euro-Atlantic Partnership Council (EAPC) succeeded the North Atlantic Cooperation Council (NACC), which was set up in 1991 just after the end of the Cold War. It is a multilateral forum focused on dialogue and consultation on political and security-related issues among Allies and partner countries. The EAPC brings together the 29 Allies and 21 partner countries. It provides the overall political framework for NATO's cooperation with partner countries in the Euro-Atlantic area, and for the bilateral relationships developed between NATO and individual partner countries under the Partnership for Peace (PfP) programme. The topics under discussion have included crisis-management and peace-support operations; regional issues; arms control and issues related to the proliferation of weapons of mass destruction; international terrorism; defence issues such as planning, budgeting, policy and strategy; civil emergency planning and disaster preparedness; armaments cooperation; nuclear safety; civil-military coordination of air traffic management; and scientific cooperation.

Topic A: ESCALATING TENSIONS IN THE BALTICS

NATO's post-Cold war evolution has been strongly influenced by events in the Balkan and the Baltic regions. While the Alliance continues to expand its areas of strategic interest and engagement, the Baltics remain a region of special concern, especially in light of recent Russian activity.

As part of NATO's eastward expansion after the Cold War, the Baltic countries joined the Alliance in 2004. The Baltics have always been a vulnerable region as they are geographically separated from nearly all other NATO states and have modest military might. From the onset, military planners understood that NATO would have to commit substantial resources to properly defend the region from Russian aggression. At the time, NATO states were unconcerned with this vulnerability, as they believed Russia to no longer be a threat. Consequently, instead of making the costly outlays required to protect the Baltic states, European NATO states cut their defense budgets.

Today, Russia's illegal annexation of Crimea in March 2014 and its subsequent military actions in Ukraine have led transatlantic policy-makers to reassess collective defence arrangements across NATO's eastern flank. Consequently, the security of NATO's Baltic member states of Latvia, Lithuania, and Estonia is of increasing concern.

Russian aggression in the Baltic region has increased substantially over the past five years. In 2014, Russian intelligence officers kidnapped an Estonian intelligence officer from Estonian territory.[1] Russian aircrafts have been conducting frequent intrusions into the air space of NATO countries and have had several close encounters with US and NATO ships and aircrafts operating in the Baltic and Black Sea regions. Russia has threatened nuclear strikes against NATO countries and Sweden and Finland should they join NATO.

Furthermore, there have been increased Russian cyber operations in the Baltic Region. Suspected Russian-backed hackers have launched exploratory cyber-attacks against the energy networks of the Baltic states, raising security concerns amongst NATO members. Lithuania, Latvia and Estonia are all locked into Russia's power network and at the end of 2015, hackers attacked an Internet gateway used to control a Baltic electricity grid, disrupting operations.[2] Although it did not cause blackouts, there were concerns that hackers had simply been dormant, as in Ukraine, hackers had infiltrated the grids for about six months before the lights went out. Suspected Russian-backed hackers had also targeted a Baltic petrol-distribution system at around the same time in an unsuccessful cyber-attack that aimed to cause widespread disruption in petrol deliveries. In both cases, hackers targeted network communication devices, serial-to-ethernet converters (STEC), which link sub-stations to central control. At the present time, NATO does have not provisions to protect the Baltic region from cyber-attacks.

[1] Stephen Jewkes and Oleg Vukmanovic, "Suspected Russia-Backed Hackers Target Baltic Energy Networks," *Reuters*, May 11, 2017, https://www.reuters.com/article/us-baltics-cyber-insight/suspected-russia-backed-hackers-target-baltic-energy-networks-idUSKBN1871W5.
[2] Jewkes and Vukmanovic, "Suspected Russia-Backed Hackers Target Baltic Energy Networks."

Nonetheless, there are talks underway for a unified strategy to counteract hybrid warfare tactics.

In response to a changed security environment, Allied leaders decided to enhance NATO's military presence in the eastern part of the Alliance at the Warsaw Summit in 2016. Since then, four multinational battlegroups totaling approximately 4,500 troops have deployed to the Baltic nations and Poland.[3] The four battlegroups are one part of the Alliance's response to Russia's use of force against its neighbours and its military build-up in the Baltic region and beyond. NATO is also strengthening its multinational presence in the Black Sea region, based around a Romanian-led multinational framework brigade. Additionally, the Alliance has tripled the size of the NATO Response Force to 40,000 and set up eight small headquarters (NATO Force Integration Units) to facilitate training and reinforcements.[4]

At the NATO Wales Summit in 2014, the Baltic States also broadly welcomed the deterrence measures agreed to form the Readiness Action Plan (RAP). The RAP ensures the Alliance is ready to respond swiftly and firmly to new security challenges emerging from Russia. A core feature of the RAP is the 5000-strong Very High Readiness Joint Task Force (VJTF) created within the NATO Response Force (NRF). This is the most significant reinforcement of NATO's collective defence since the end of the Cold War. Nevertheless, many in the Baltics see it as a work in progress.

The assurance measures under the RAP include a series of land, sea, and air activities throughout the territory of NATO Allies in Central and Eastern Europe. These measures are designed to reinforce state defences, reassure populations, and deter potential Russian aggression. All 29 Allies are contributing to these measures on a rotational basis.

In response to Russia's increased military exercises, which included unannounced exercises simulating the use of nuclear weapons in an invasion of the Baltics, NATO has increased the number of military exercises it organises as well. Military exercises provide important opportunities to improve the ability of Allies and partners to work together, and are a valuable demonstration of NATO's readiness to respond to potential threats.

Since May 2014, NATO has increased the number of fighter jets patrolling the Baltic states and in December 2015, a further package of tailored assurance measures

[3] North Atlantic Treaty Organization, "NATO Battlegroups in Baltic Nations and Poland Fully Operational," North Atlantic Treaty Organization, last modified August 28, 2017, accessed January 6, 2018, https://www.nato.int/cps/en/natohq/news_146557.htm.
[4] North Atlantic Treaty Organization, "NATO Battlegroups," North Atlantic Treaty Organization.

was agreed for Turkey, including regular air and marine surveillance.[5] These measures were put in place to support Ankara due to the rising tensions with Russia.

To provide assurance at sea, NATO deploys a number of multinational maritime forces including the Standing NATO Mine Counter-Measures Group patrolling the Baltic Sea and the Eastern Mediterranean, and an enlarged Standing NATO Maritime Group conducting maritime assurance measures in addition to counter-terrorism patrols.

These forces and the measures in place are a defensive and proportionate deterrent force, fully in line with NATO's international commitments. They send a clear message that an attack on one member would be met by troops from across the Alliance.

Questions for Discussion:

1) How can NATO allies improve the Readiness Action Plan to better meet the needs of the Baltic region?
2) Is there a better alternative to the Readiness Action Plan? Should a different plan be implemented to address the concerns within the Baltic region, in particular?
3) Should countries who are not NATO members, such as Finland and Sweden, be invited to participate in Baltic reassurance initiatives?
4) Should the Readiness Action Plan include provisions for cybersecurity? If so, what kinds of provisions and how would they be ensured?

Further Reading:

RAND Corporation: Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics
https://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1253/RAND_RR1253.pdf

NATO: Securing the Nordic-Baltic Region
https://www.nato.int/docu/review/2016/also-in-2016/security-baltic-defense-nato/EN/index.htm

[5] Robin Emmott, "Exclusive: NATO Agrees Turkey Air Defense Package, Seeks 'Predictability," *Reuters*, December 18, 2015, https://www.reuters.com/article/us-mideast-crisis-turkey-nato-exclusive/exclusive-nato-agrees-turkey-air-defense-package-stoltenberg-idUSKBN0U123520151218.

Reuters: Suspected Russia-backed Hackers Target Baltic Energy Networks
https://www.reuters.com/article/us-baltics-cyber-insight/suspected-russia-backed-hackers-target-baltic-energy-networks-idUSKBN1871W5

Carnegie Endowment for International Peace: The New NATO-Russia Military Balance: Implications for European Security
http://carnegieendowment.org/2017/03/13/new-nato-russia-military-balance-implications-for-european-security-pub-68222

NATO: Readiness Action Plan
https://www.nato.int/cps/ua/natohq/topics_119353.htm

Topic B: RESPONDING TO CYBER THREATS TO INFRASTRUCTURE

Recent years have seen an escalating frequency and severity of cyber attacks. These attacks are diverse in their origins, targets, and methods. A disturbing recent trend however has seen attacks targeting critical infrastructure. Ukraine has seen multiple attacks on its power grid, resulting in significant outages during the winter, as well as a steady barrage of attacks to private and public organizations.[6] While the recent attacks have been mostly contained, a protracted attack could have devastating consequences. If a cyberattack is able to disable or severely damage the energy infrastructure (especially during the winter) of a country, significant outages could result in devastating knock-on effects throughout the economy. The resulting material and economic costs to the country could be extremely high, while leaving the country very vulnerable during an attack.

The scope of cyber threats are not limited to the infrastructure of one country. Cyber attacks have had impacts worldwide. Due to the globalised nature of these threats, problems faced by one country cannot be dismissed as local to that country alone, but should rather be seen as potential threats to any country. The increasing reach of computing and the internet into all variety of activities has increased the level of threat posed by potential cyber attacks. The financial sector, critical infrastructure, transportation, government, and of course the military are all potential targets of cyber attack.

Cyber attacks could come from a varied nature of sources, with varied targets and goals. Many attacks, such as the recent WannaCry attack, are focused on extracting ransom. These are international criminal attacks that, while their motivations may be

[6] Andy Greenberg, “How An Entire Nation Became Russia's Test Lab for Cyberwar,” *Wired*, June 20, 2017.

somewhat predictable, their potential to do damage on a global level are very high. The WannaCry virus appeared suddenly across Europe and Asia in May 2017, locking individuals out of their computers unless they paid a bitcoin ransom. Hundreds of organizations and institutions were affected, including financial institutions and the UK's National Health System. Luckily however, the WannaCry virus was equipped with a "kill switch" that ended the virus' spread after it had only raised $50 000 in ransom. Had the "failsafe" for WannaCry not been discovered, or if it had simply not included one at all, the financial damages could have been much higher.

On the other hand, attacks may be politically motivated. These could be perpetuated by state or non-state actors, though pulling off an effective cyber attack requires a significant investment. These attacks are focused on high-impact targets in a country selected to advance a political agenda. The Stuxnet virus was one such political attack, as it targeted Iran's nuclear enrichment facilities, destroying one-fifth of Iran's nuclear centrifuges in 2009 with a sophisticated malware attack.[7] Attacks on Estonia and Georgia in 2007 and 2008 targeted government, media, and financial websites with denial-of-service attacks.[8] [9] The attacks were determined to be Russian in origin, and occured during political disputes with Russia. Official Russian statements laid the blame on rogue government workers. The recent attack on Ukraine's power grid, with Russian origins and no ransoms extracted, are another example.

Whether the motives for a cyber attack are political or monetary in nature, similar challenges to a country's security apply. Attacks can do significant damage in a short period of time, and in the event of a protracted attack, could have humanitarian impacts. While an attack might focus on one country, it is very easy for the attack to spread, or for knock-on effects to spread to other countries. For example, an attack targeting a country's power grid could interrupt the flow of natural gas through that country to its neighbours. Attacks can also come from any part of the world at any time due to the nature of the technology. Due to the shared impacts of the threat, and the global nature of its origins, international cooperation is a necessary component of any country's policy on cyber security.

[7] Paul Szoldra, "A new film gives a frightening look at how the US used cyberwarfare to destroy nukes," *Business Insider*, July 7, 2016.
[8] Travis Wentworth, "How Russia may have attacked Georgia's internet," *Newsweek*, August 22, 2008.
[9] Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian*, May 7, 2007.

Questions for Discussion:

1) What new areas may be threatened by cyber attacks now that weren't in the recent past, and what areas may be a target in the near future?
2) How can non-state actors be effectively deterred from committing cyber crime?
3) Can international treaties be established on cyber warfare?
4) What steps can NATO take to cooperate with its European partners to counter cyber threats?
5) Can NATO and Russia work together to de-escalate the threat of cyber attacks?

Further Reading:

Wired: How An Entire Nation Became Russia's Test Lab for Cyberwar
https://www.wired.com/story/russian-hackers-attack-ukraine/

Microsoft: The Need for a Digital Geneva Convention
https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

US News: Former CIA Director: Cyber Attack Game-Changers Comparable to Hiroshima
https://www.usnews.com/news/articles/2013/02/20/former-cia-director-cyber-attack-game-changers-comparable-to-hiroshima

Guardian: WannaCry ransomware has links to North Korea, cybersecurity experts say
https://www.theguardian.com/technology/2017/may/15/wannacry-ransomware-north-korea-lazarus-group

Threatpost.com: Vulnerable Radiation Monitoring Devices Won't be Patched
https://threatpost.com/vulnerable-radiation-monitoring-devices-wont-be-patched/126967/

Wired: An Unprecedented Look at Stuxnet, the World's First Digital Weapon
https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Topic C: CO-OPERATING ON NUCLEAR SAFETY

In September 2017, European radiation monitoring stations detected trace amounts of the radioactive isotope ruthenium-106 in the atmosphere.[10] Ruthenium-106 is produced as a by-product of nuclear fission. While the amount detected in the atmosphere over Europe is not particularly dangerous, it points to an inadvertent release of radioactive materials by a nuclear site, which is cause for concern.[11] The Russian government eventually confirmed that it had detected very high concentrations of Ruthenium-106 in September, in the Ural Mountains.[12] This was detected in a region near the Mayak plant, a large nuclear processing complex in Russia, where a disastrous nuclear accident occurred in 1957.[13]

While Russian authorities have maintained that there is no need for alarm, and that Mayak was not the source of the radiation spike, this incident underscores the potential shared impacts of a nuclear disaster. Just as the Chernobyl disaster caused contamination and fallout beyond the borders of the Soviet Union, an event at a nuclear facility within any partner country could have wide-ranging impacts on other partner countries.

A Russian-financed nuclear power plant is currently under construction in Astravets, Belarus, on the border with Lithuania. The location of this plant, less than 50km from Vilnius, the capital of Lithuania, has caused significant friction between Lithuania and Belarus.[14] Lithuania is concerned about the lack of consultation over the plant's location, and potential safety issues. Belarus maintains that it has the right to develop its energy infrastructure, and that its plant is being built according to proper safety standards.

While it would be ideal for the partner countries to resolve this particular dispute, the committee is tasked with avoiding similar disputes in the future, and potentially coming to agreement on nuclear safety standards. Russia is backing several new reactors in multiple states, including Hungary.[15] The committee will need to consider whether this

[10] Matthew Luxmoore and Alan Cowell, "Russia, in Reversal, Confirms Radiation Spike", *The New York Times*, November 21, 2017.
[11] Emily Chung, "What's ruthenium-106? What you need to know about Russian radiation," *CBC,* November 21, 2017.
[12] Luxmoore and Cowell, "Russia, in Reversal, Confirms Radiation Spike".
[13] Miss Cellania, "The Kyshtym Disaster: The Largest Nuclear Disaster You've Never Heard Of," *Mental Floss*, November 12, 2015.
[14] Reid Standish, "Lithuania, Leery of Moscow, Spars With Belarus Over Nuclear Reactor," *Foreign Policy*, October 31, 2017.
[15] Sara Stefanini and Nicholas Hirst, "Hungary's Russian-built nuclear plant powered by politics in Brussels," *Politico*, November 22, 2017.

might have negative impacts on relations between partner countries, and whether these facilities are built to adequate standards. Due to the shared cross-border risk potential of nuclear energy, partner countries will need to work together to resolve issues and to ensure transparency in their infrastructure projects.

Questions for NATO to consider:

1) Are new Russian-backed plants being built in accordance with IAEA standards?
2) Should partner countries take the concerns of neighbouring countries into account when developing their energy infrastructure?
3) At what point should countries be concerned about nuclear installations in neighbouring countries?
4) Are current international nuclear safety regulations sufficient?

Further Reading:

Foreign Policy: Lithuania Spars With Belarus Over Nuclear Reactor
http://foreignpolicy.com/2017/10/31/lithuania-leery-of-moscow-spars-with-belarus-over-nuclear-reactor/

Radio Free Europe Belarus Proceeding With Russian-Built Nuclear Plant Despite Accidents, Quake Worries, And Neighbors' Objections
https://www.rferl.org/a/belarus-astravets-nuclear-plant-lithuania-quake-fears/28749653.html

IAEA: "Site Survey and Site Selection for Nuclear Installations"
http://www-pub.iaea.org/MTCD/publications/PDF/Pub1690Web-41934783.pdf

NY Times: Russia, in Reversal, Confirms Radiation Spike
https://www.nytimes.com/2017/11/21/world/europe/russia-nuclear-cloud.html

IAEA: "Convention on Early Notification of a Nuclear Accident"
https://www.iaea.org/publications/documents/treaties/convention-early-notification-nuclear-accident

Politico: "Hungary's Russian-built nuclear plant powered by politics in Brussels"
https://www.politico.eu/article/hungarys-russian-built-nuclear-plant-powered-by-politics-in-brussels/