Republic of Estonia

Positions for the North Atlantic Treaty Organization

I. Addressing the resurgent insurgency in the Islamic Republic of Afghanistan

The Republic of Estonia, along with all fellow North Atlantic Treaty Organization (NATO) member states, is increasingly concerned at the reemergence of violent insurgencies in the Islamic Republic of Afghanistan and the threats faced by the legitimate government in the state. Combined with regional instability stemming from international terrorist networks such as the Islamic State (ISIS/ISIL) and escalating tensions between major regional powers in Iran, Pakistan, and Saudi Arabia, Afghanistan remains a global flashpoint in regards to international terrorism. The International Security Assistance Force (ISAF), started in 2001 and approved by the United Nations Security Council (UNSC), succeeded in establishing a sovereign Afghan state and reducing the power of Al Qaeda, the Taliban, and other factional groups in the region. The most difficult NATO mission to date, at its height the ISAF force included over 120,000 troops from dozens of NATO member states and allies. Ended in 2014, the ISAF was succeeded by the Resolute Support Mission (RSM), which aims to train, advise, and assist Afghan Security Forces and other state institutions as they continue to root out radical groups. Currently, RSM numbers just under 20,000 troops from 39 NATO allies and partner states.

As one of the chief contributors to NATO and an active member since its ascension to the body in 2004, the Republic of Estonia recognizes the power of the institution and the increased capabilities of each Member-State when working in tandem. The Republic of Estonia has worked with the body since its role as a partner state, and has contributed soldiers to assist NATO missions in Kosovo, Afghanistan, and Iraq to combat extremism and promote internationalism. The Republic of Estonia is proud to house the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) and believes the relationship between NATO and the Republic of Estonia to be integral success for both parties. The Republic of Estonia has worked with fellow European Union (EU) Member-States to combat extremism and terrorism in Europe, and recognizes the global threats regionalized crises cause.

The Republic of Estonia believes it is integral NATO reassert its mission in Afghanistan and increase its support for state institutions. While it is necessary for Afghan forces to lead the effort to combat extremism in the region, Estonia strongly advocates for the continued NATO mission in Afghanistan in order to successfully complete all peacemaking and peacebuilding operations. In that spirit, Estonia remains committed to the mission of the ISAF and is willing to provide the appropriate number of personnel and equipment necessary to fulfill our obligation as a member of this mission. The Republic of Estonia would also recommend that NATO implement new technological solutions with two primary intentions; the disruption of insurgent communication networks and the security of local Afghan allied communication systems. Furthermore, the Republic of Estonia firmly believes in the ongoing Afghan-lead peace talks currently underway as being the best possible solution to the conflict in Afghanistan; Estonia urges its fellow Member-States, as well as its NATO allies, to continue in support of this diplomatic process and facilitate its completion through whatever avenues deemed appropriate.

II. Improving Cyber Security in response to increased hostile interference

The Republic of Estonia is gravely concerned with the continued prevalence of cyber-attacks coordinated by hostile foreign actors, specifically the Russian Federation, which target the informational security of both NATO allies and fellow UN Member-States. These attacks have resulted in the unlawful theft of information, interference in domestic politics, and the collapse of critical communication networks; all of which have generated increased uncertainty and instability within the targeted state. The Republic of Estonia recognizes this threat and places it as a high priority; in 2007, a series of crippling cyber-attacks organized by Russian-based hackers struck several key sectors of Estonia's communication networks. Known as a Distributed Denial of Service (DDoS) attack, it compromised critical infrastructure and left the country defenseless. Similar attacks have followed suit, with the Russian Federation the primary actor involved; during the Russian invasion of Georgia in 2008 similar attacks were used to cripple key networks in support of the conventional invasion. Incidents in Ukraine included interference in the 2014 Ukrainian presidential election, shortly before the Russian annexation of Crimea. Election interference in the 2016 United States presidential election and the 2018 North Macedonia referendum have also allegedly been orchestrated by Russian-backed sources.The continued interference in the critical systems of NATO allies and partners is an ongoing issue that Estonia strongly believes should be placed at the highest priority.

After the 2007 cyber-attacks, the Republic of Estonia has placed itself as a leader in cyber-security within both NATO and the global community at large. On the international level, Estonia has supported numerous actions taken by the UN and NATO in regards to improving cyber-security. The 2018 Global Cybersecurity Index, created by the United Nations International Telecommunication Union (ITU), ranked Estonia fifth in the world in commitment to cybersecurity, with proficient scores in the technical category being representative of Estonia's continued progress in cybersecurity research. Furthermore, the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) is based in Estonia's capital, Tallinn, and serves as the premier cyber-security apparatus of NATO. Estonia was a major figure in the development of the Tallinn Manual, which outlines and details the relationship between international law and the cyber-warfare. In 2017, Estonia hosted Locked Shields, the world's largest cyber defense exercise, with over 800 participants from 25 different countries all engaged in simulations of cyber-attacks. Estonia is also a leader in innovative cyber-security programs; domestically, Estonia has created a Volunteer Cyber Defense Unit, composed of Estonian citizens who specialize in cyber-security, which operates in concert with other branches of the Estonian Defence League and the Estonian military.

The Republic of Estonia posits that cyber-security is the greatest current threat to the collective defence of NATO Member-States and partners, and as such advocates for a greater allocation of resources be dedicated to the continued research and development of new and effective cyber-security solutions. Estonia strongly urges its fellow Member-States to adopt similar domestic cybersecurity policies, specifically in regards to volunteer cyber defense groups that promote interaction and unity in the public and private sectors. Furthermore, the Republic of Estonia recognizes and condemns the actions of hostile actors, specifically the Russian Federation, for their role in instigating and sponsoring unrestrained cyber warfare; Estonia calls upon its allies to join in this condemnation, as well as to begin a serious investigation into these groups, with cooperation from international law enforcement agencies, and eliminate this threat.