TECHNOLOGY FOR GLOBAL SECURITY

RUSSIA'S NC3 AND EARLY WARNING SYSTEMS

TECHNOLOGY FOR GLOBAL SECURITY SPECIAL REPORT

LEONID RYABIKHIN

Holds Research Positions in the Russian Diplomatic Academy and in the Institute of World Economy and International Relations

July 11, 2019

RUSSIA'S NC3 AND EARLY WARNING SYSTEMS

LEONID RYABIKHIN
JULY 11, 2019

I. INTRODUCTION

In this essay, Leonid Ryabikhin argues that distrust, misunderstanding and concern prevail in US/NATO and Russia relations "which increases the risk of unintended or accidental conflict. Human or technical mistakes and a variety of natural events can cause the failure or malfunction of technical systems and errors in decision making. The absence of contacts between the United States and Russian military and the failure to reach new agreements while existing agreements collapse worsens an already dangerous situation."

Leonid Ryabikhin holds research positions in the Russian Diplomatic Academy and in the Institute of World Economy and International Relations. In 1989, he joined the Committee of Soviet Scientists for Peace Against Nuclear Threat and the Committee of Scientists for Global Security and Arms Control where he is Executive Secretary. He also served in the USSR Air Force.

Acknowledgments: The workshop was funded by the John D. and Catherine T. MacArthur Foundation. This report is published simultaneously here by the Nautilus Institute and is published under a 4.0 International Creative Commons License the terms of which are found here.

The views expressed in this report do not necessarily reflect the official policy or position of Technology for Global Security. Readers should note that Technology for Global Security seeks a diversity of views and opinions on significant topics in order to identify common ground.

Banner image is by Lauren Hostetter of Heyhoss Design

CITATION

Ryabikhin Leonid, "Russia's NC3 and Early Warning Systems," Tech4GS Special Reports, July 11, 2019, https://www.tech4gs.org/nc3-systems-and-strategic-stability-a-global-overview.html

II. TECHNOLOGY FOR GLOBAL SECURITY SPECIAL REPORT

LEONID RYABIKHIN

RUSSIA'S NC3 AND EARLY WARNING SYSTEMS

JULY 11 2019

Summary

During the Cold War, the Soviet Union and the United States accumulated enormous nuclear arsenals and possessed about 90 percent of all nuclear weapons in the world. China and formally unrecognized nuclear states India and Pakistan built up and continued to modernize their nuclear weapons and its means of delivery. The former Soviet Union (USSR) then Russia and the United States concluded a number of agreements on nuclear forces reduction. Both nuclear superpowers lowered their reliance on nuclear arms. After the Soviet Union dissolved and its economy stagnated, Russian conventional forces degraded. Russia's defense budget reached its minimum. Consequently, Russia's leadership considered nuclear deterrence to be the cornerstone of Russia's security policy. But Russian nuclear strategic forces also suffered from the shortfall in the defense budget. Strategic arms were aging and needed modernization or replacement. Russia's missile early warning system was in bad shape. Several Soviet-era early warning (EW) radars were no longer on Russian territory. Most of EW satellites reached or were close to the end of their operational life. With economic recovery, Russia invested significant financial resources into an ambitious rearmament. Russia already deployed new ICBM complexes, cruise missiles, and started to modernize its NC3 and EW systems. At the same time, tension rose in US/NATO and Russia relations over the Ukrainian crisis, Syria, etc. Now, distrust, misunderstanding and concern prevail, which increases the risk of unintended or accidental conflict. Human or technical mistakes and a variety of natural events can cause the failure or malfunction of technical systems and errors in decision making. The absence of contacts between the United States and Russian military and the failure to reach new agreements while existing agreements collapse worsens an already dangerous situation.

NC3 in the Russian Federation

On December 1, 2014, the National Defense Command and Control Center (NDCCC) became operational in the Russian Federation. Over the previous fifty years, the Central Command and Control HQ of the Armed Forces General Staff carried out the command and control of Soviet/Russian Armed Forces.

The NDCCC provides the management over all spheres of Armed Forces activity. It has three major control centers:

- Nuclear Strategic Forces Command and Control Center
- Combat Command and Control Center
- Command and Control Center over "day-to-day" activity of the State military organization and other forces and units besides the Ministry of Defense (MoD)

The Nuclear Strategic Forces Command and Control Center manages the use of nuclear weapons under the decision of the state's highest political-military leadership. Traditionally Russia has a nuclear triad

which includes Strategic Rockets Forces (RVSN), Air Force Strategic Aviation, and NAVY Nuclear Ballistic Missile Submarines (SSBN).

Command and Control System of the Russian Strategic Rocket Forces

The Strategic Rockets Forces are the major component of Russia's nuclear deterrence capability. By the end of the 1950s different types of ballistic missiles (BM) had been developed in the USSR. In 1958 the first combat unit of intercontinental ballistic missile (ICBM) R-7 under the name "Object Angara" was deployed in the Soviet Armed Forces. R-7 had a range of 8000 km and was the first Soviet ICBM that could reach the continental part of the United States. On December 17, 1959, Russia established the Strategic Rocket Forces as a new Service of the Armed Forces in accordance with the "top secret" decision of of the USSR Council of Ministers #1384-615 "Establishing the Position of Commander-in-Chief of the Rocket Forces in the USSR Armed Forces." On December 31, 1959, Russia formed the command and control system of the SRF including the Main Command and Main Staff. Deputy Defense Minister Marshal of Artillery M. Nedelin became the first Commander-in-Chief of the Soviet SRF. By the end of 1960 10 rocket divisions armed with intermediate range BMs (2.3 Mt warhead) had been deployed in the Western part and Far East of the Soviet Union. Even in 1986 the SRF had 112 R-12 launchers. The last R-12 was destroyed under Intermediate-Range Nuclear Forces Treaty. Only one division was armed with ICBM R-7. This ICBM was on combat duty until 1968.

Initially the first rocket units used the rather simple Control and Command System, which was used in artillery in the Reserve of Supreme Command. With time Russia improved and modernized the Command and Control System with new requirements and the introduction of innovative technologies like electronic computers, communication systems, and space means.

Now the Russian SRF have their own Main Command, Main Staff, and Central Command Post with a Communication Center, Computing Center, and other departments and services.

The combat capability of the Russian SRF depends not only on the number of BMs but also on the effectiveness of Command and Control. The C3 system must deliver fast and reliable information exchange between all structural elements of the SRF and the transfer of commands to all BM combat positions. The Central Command Post (CCP) of SRF provides for centralized combat management by all duty forces. Four identical shifts are constantly on combat duty. CCP also includes management, information unit, combat readiness preparation and control and coordination of other Command Post units, analytical groups, and other units. CCP is situated in the small town of Vlasiha (Moscow District) in a bunker at a depth of 30 m. The special equipment provides CCP with constant communication with all SRF combat posts with almost 6 thousand officers on duty.

The Combat Management Automated (computer aided) System (CMAS) of Nuclear Strategic Forces has the name "Kazbek." Its portable terminal "Cheget" is known as "nuclear briefcase." Only three people in the Russian political-military leadership have such briefcases—the President as the Supreme Commander, the Minister of Defense, and the Chief of General Staff. These briefcases are used for the transmission of special code to Command Posts of the SRF, which permit the use of a nuclear weapon. Permission takes place when code is received from at least two terminals.

With deployment of the ISBM System "Yars" the SRF employs a fourth generation CMAS. The initial elements of the fifth generation CMAS were scheduled for introduction after 2016. The new CMAS will allow transmission of combat orders directly to BM launchers. It can also provide inflight targeting for the modern types of BM ("Topol-M", "Yars" and "Bulava"). Such operation is unavailable for the old types of BM—"R-36" (P-36) and "UR-100" (УР-100).

The Russian SRF are able to ensure the launch of a nuclear missile strike, even in the case of a first massive nuclear attack on Russia, when command chain and combat management systems are destroyed and personnel at missile units are dead. According to the Russian MoD official site, the Special Command and Control System known by the name "Perimeter" was developed and introduced into the SRFs in 1986. This is an automated complex for managing a massive retaliatory nuclear strike by the SRF. In Western media it is known as "the Dead Hand." Nothing is known about this system from official sources and what is known derives from rumors, mostly reported in Western media. For many years, all information about this system was kept "Top Secret." In 2011 General S. Karakayev, Commander-in-Chief of the Russian SRF, confirmed in an interview with one of the central Russian newspapers that "Perimeter" exists and continues to be on combat duty. "Perimeter" has been developed as the duplicate command and control system for all forces armed with nuclear weapons and is designed to guarantee the launch of BM from silos and submarines if the "Kazbek" System and the combat command and control systems of the SRF, NAVY, and Air Force are destroyed.

The "Perimeter" system's characteristics and capabilities are unknown. According to some unconfirmed information the system's central component of program and command complex is based on artificial intelligence software. This complex monitors the situation using many parameters from its own sensors. After Russia concludes that a nuclear BM occurred and decides to start a retaliatory attack, it launches special command ballistic missiles 15A11 are launched (the 15A11 was a special modification of multiple warhead UR-100 ICBM). Using powerful onboard transmitters, inflight command BMs relay the order to launch all surviving ICBMs and submarine launched ICBMs.[1]

Use of Nuclear Weapon: Evolution of Russia's Nuclear Doctrine

The growing accumulation of nuclear arsenals during the Cold War led to the conclusion that large-scale use of nuclear weapons was unacceptable. Such understanding led to the doctrine that the mission of nuclear weapons is to deter their use by a potential adversary. If the Soviet-era military doctrine on nuclear weapons was primarily aimed at propagating deterrence, today's Russian military doctrine has more interconnections with real military strategic and operational plans.

The nuclear policy of Russia is formally articulated in all military doctrines of the Russian Federation. At the same time, it must be noted that none of the countries that are official members of the Treaty on the Non-Proliferation of Nuclear Weapons have made public their operational plans for combat use of nuclear forces.[2] The degradation of Russian conventional forces in the 1990s and 2000s due to economic stagnation forced political and military leadership to consider nuclear deterrence as a cornerstone of the Russia's security policy.

[1] For more information see www.modernarmy.ru/article/460/rvsn

[2] Nuclear Deterrence and Non-Proliferation. Ed. by A. Arbatov and V. Dvorkin. Carnegie Moscow Center.2006

The major task of Russian SNFs was originally to supply the appropriate level of nuclear deterrence. However, the Russian post-Soviet nuclear policy depended on nuclear deterrence. In the beginning of the 1990s Russia's nuclear deterrence reliance was low. At first, the USSR's "no-first-use" commitment of nuclear weapons was confirmed in the Russian Federation's draft military doctrine in 1992 but was dropped from the military doctrine in 1993 Many military experts considered the "no first use" commitment propaganda. In fact, there were no plans to use a nuclear weapon in preventive strikes in the text of doctrine. As one expert noted, the document "did not assign any specific missions supposed to respond."[3]

The military doctrine issued in 2000 stated that Russia retains its status as a nuclear nation and feels the need to possess a nuclear deterrent "guaranteed to inflict the intended damage on an aggressor under any conditions." It stated that "Russian Federation reserves the right to use nuclear weapons in response to the use of nuclear weapons and other types of weapons of mass destruction against it and/or its allies, as well as in response to a large-scale aggression using conventional weapons in situations that are critical to the national security of the Russian Federation."[4] But like the Military Doctrine of 1993, that issued in 2000 did not posit planned use of a nuclear weapon in preventive strikes.[5] The growing "reliance on nuclear weapons was seen as a "fix" intended to provide security until conventional forces were sufficiently modernized and strengthened."[6]

The military doctrine issued in 2010 stated that "the Russian Federation reserves the right to utilize nuclear weapons in response to the utilization of nuclear and other types of weapons of mass destruction against it and (or) its allies, and also in the event of aggression against the Russian Federation involving the use of conventional weapons when the very existence of a state is under threat." This doctrine declares that Russia can use a nuclear weapon:

- as retaliatory nuclear strike against first use of nuclear weapon by aggressor
- as a first use of a nuclear weapon as retaliation against BW or/and CW use by aggressor
- as a first use of nuclear weapon against aggression by conventional forces and arms posing an existential challenge

Being prepared to deliver a retaliatory nuclear strike is common paradigm adhered to by all nuclear states and a premise of deterrence doctrine. Any nuclear state contemplating nuclear aggression against a nuclear-armed state must assume that a retaliatory nuclear strike is inevitable. Thus, the common understanding among nuclear commanders is that nuclear war would be suicidal. That is why the probability of the large-scale war between major nuclear powers is very small, leaving aside muscle-flexing bravado and warlike rhetoric.

It should be noted that the risk of large-scale use of chemical or biological weapons against Russia is extremely low. It is impossible to imagine that the United States, NATO, or China would use such

[3] Nikolai Sokov. "The Evolving Role of Nuclear Weapons in Russia's Security Policy", in ed. William Potter and Cristina Hansell, Engaging China and Russia on Nuclear Disarmament, CNS Occasional Paper 15, April 2009, pp. 76–77.
[4] Military Doctrine of the Russian Federation. Nezavisimaya Gazeta. April 22, 2000.
[5] Yu. Baluevsky. New meaning of military doctrine. *Military Review*. http://topwar.ru/62298-novye-smysly-voennoy-doctriny.html
[6] Nikolai Sokov, "Russia's 2000 Military Doctrine", revised July 2004, www.nti.org

weapons against Russia. All responsible states are members of the chemical and bio-weapons conventions, including the above-mentioned nuclear weapons states, and eliminated or nearly eliminated all such capacities (that is, the United States and Russia retain some residual break-out capacity). Only a few states still possess chemical weapons arsenals, but only on a limited scale that could never justify Russian nuclear retaliation to a chemical and biological weapon that much weaker adversaries could theoretically launch. Furthermore, biological weapons can be used so clandestinely that it is hard to identify the attacker, which might be an aggressor-state or a non-state actor. And if attribution is impossible or that attack is anonymous, surely it is impossible to use a nuclear weapon in response to biological attack?

Russia's 2010 military doctrine posits the first use of nuclear weapons against the overwhelming conventional forces attacking Russia when the very survival of a state would be at stake. Many experts see the roots of this declaration in Russian perception of US/NATO superiority in conventional forces. The Russian strategists and military authorities worry about US superiority in all types of so called "smart weapons" and constantly growing potential of this type of arms, which already reach strategic levels. The Russian military recognize that conventional long-range, precision-guided weapon systems can undermine Russia's strategic nuclear capacity and ability to launch a retaliatory strike after an attack by conventional strategic weapons. The US Defense Department's Conventional Prompt Global Strike Program provoked the Russian military leadership to search for a countervailing response. Russia also launched the development of its own "smart weapons" but reaffirms its adherence to the policy of nuclear deterrence. The 2010 military doctrine does not mention "pre-emptive devastating strike as prevention of aggressor's nuclear attack," "assured destruction," or "devastating retaliation" contained in earlier statements. In general, the 2010 doctrine reflects a more restrained attitude to the role and task of nuclear weapons compared with the doctrine issued in 2000. The task of "aggression de-escalation by threat or direct strikes of different scale with conventional and/or nuclear weapons" has been excluded from the 2010 doctrine. Their conception of "measured combat use of separate components of Strategic Deterrent Forces" is nowhere to be found.

The military doctrine issued in 2014 states that "The Russian Federation reserves the right to use nuclear weapons in response to use of nuclear and other types of weapon of mass destruction against it and (or) its allies, and also in the event of aggression against the Russian Federation involving the use of conventional weapons when the very existence of the state is under threat."

Today military and security experts discuss the possible use of nuclear weapons to deter massive cyberattack on national Command and Control Systems, EW Systems and other national critical infrastructure facilities. Such attack can be considered as preliminary action before the massive devastating nuclear strike. This is not very new and such discussion has been started many years ago when experts began to consider cyber weapons as a new type of weapon of mass destruction along with nuclear, chemical, and biological weapons. But many experts are skeptical that Russia would ever use nuclear weapons in response to chemical or bio weapons. And, as in the case of bio-weapons, there are many reasons to not employ nuclear weapons in scenarios of cyber attack including attribution problems.

Ballistic Missile Early Warning System

In 1967 the decision to develop a prototype of the EW complex was made. The goal was to detect the incoming ballistic missiles flying from the northern direction. The EW complex was developed and tested in a short timeframe. In August 1970 the EW complex was fielded and became operational. The complex included two "Dnepr" radars near Murmansk and Riga and the Command Post near Moscow. At the same time Special EW Division was formed. Then it was transformed into the Third Special (independent) EW Army, which became the basis of Missile and Space Defense and included the military units of Ballistic Missile Defense System (BMD), Space Defense, and Space Surveillance System.[7]

The major task of the Ballistic Missile Early Warning System (BMEWS) is *"*Providing the top political-military leadership with complete, timely and reliable data on the current state of missile situation throughout the near-Earth space and, especially, on its changes posing a threat to the security of the country."

BMEWS is the major technical means of providing such information for the state political-military leadership decision to use nuclear weapons. The major requirement of the EW System is high reliability and timely reporting of data to the military-political leadership of the country.

The Soviet-then-Russian Ballistic Missile Early Warning System has been created as an important element of its overall nuclear deterrence strategic capacity, which ensures the national security of the country and strategic stability of the world. Only two states—the Russian Federation and the United States—have full scale BMEW systems. The other nuclear states are in the process of developing their own EW systems.

The Russian BMEWS is closely interrelated with the BMD and Space Surveillance System (SSS). All three systems complement one another informationally and functionally.

The creation of the BM Early Warning System was made in accordance with some conceptual provisions:

1. Continuous control in time and from any direction. This requires:

- complete radar coverage (radar barrier) along the periphery of the country
- very stringent requirements on the reliability of equipment (double-triple redundant, geographically dispersed communication, independent power supply sources)
- the absence of interruptions in the system in connection with the modernization and introduction of new objects

2. Tracking of ballistic missile from the start and along the entire route of flight (as possible). This is provided by two echelons configuration of BMEWS: space-based—BM start and active trajectory and ground-based—the final part of the trajectory.

- Ground-based echelon—VHF and UHF bands line-of-sight radars

[7] See https://structure.mil.ru/structure/forces/vks/50letRKO/sprn.htm

- Space-based echelon—satellites infra-red sensors detection system (OKO System)

3. Close information interrelation with BMD system and Space Surveillance System. BMEWS sensors are the basis for the SSS. The Catalog of the SSS reduces the level of false alarms.

4. Maximum automation of messages generation.

Partial operator participation in the decision-making process was allowed. So, initially, the OKO system was planned to introduce—in addition to the automatic channel—the visual channel with operator participation for evaluating the missile situation. Later, this operator channel was eliminated. The chief designers have defended the thesis by arguing that the decision-making algorithm is developed by high-level professionals. Then it undergoes different verifications and constant improvement. In addition, as a part of Russian BMEWS, the unique automatic subsystem was produced for monitoring the readiness, as well as for reliable evaluation of current characteristics, combat capabilities, and control of the System. The training level of an operator is essentially lower; his activity depends on the emotional state and other factors.

The notifying information has levels of threat. The decision on transferring threat levels occurs automatically. The operator reports that an automatic warning has been issued by a separate channel, and can also submit argument as to whether this information should be blocked from further reporting as in error or non-consequential.

In the 1990s the Russian BMEW System became degraded and needed deep renovation and modernization including new satellites, modern infra-red sensors, and other equipment. At the end of 2014 the Russian BMEWS had three OKO-1 satellites held over from the Soviet Union. According to "Kommersant" newspaper one of these had malfunctioned, and the other two only provided coverage for a few hours a day. Both were close to the end of their operational lifetime. But Russia is not entirely blind to BM launches in the interim period between the old and new systems, since ground-based radars also play a role in detecting incoming missiles. Satellites simply increase the speed of detection. The space-based units allow you to pinpoint the launch of an enemy missile about a minute earlier than radar stations.

Russia made sufficient investment to maintain, modernize, and upgrade the technical characteristics of its EW System including land-based and space-based echelons, launch of new satellites to replace old ones, and to reach better observation capability. Today the obsolete radars are stood down, and the modern Voronezh radars have been invented (Voronezh M and Voronezh DM), designed on the principles of "the high factory readiness" and "open architecture." The place of deployment of the new radars is the territory of Russia. The EW space echelon is being developed based on the concept of "Integrated Space System" and includes expanding the observation area and increasing the probability of BM launch allocation. The plan of further BMEWS development also includes modernizing the system command posts based on new information technologies, expanding the ability to detect and monitor new types of targets, etc.

Peculiarities of BMEW Systems Functioning

The robust and reliable functioning of all BMEW Systems is a mutual interest of all states. BMEWS are the important instrument for securing world peace, strategic stability, predictability and reduction of the risk of accidental BM launches, and unintended nuclear war. The Russian Federation and the United States have never violated their mutual agreement not to interfere into the functioning of each other's BMEW System. Many useful initiatives towards establishing wide cooperation in the security interests of both states and mankind remain to be fulfilled.

The algorithms of BMEW System operational functioning are developed on the basis of the modelling of the possible actions of the potential enemy. But the calculation results can be influenced by unskilled actions of operators, by insufficient knowledge of military and technological capabilities and actions of different states, by emergency situations of natural events, and by provocative actions, etc. It is impossible to foresee all this and write it into algorithms.

The operators of the EW System who control the system functioning can also influence the decisions resulted by the system calculation in automatic mode. The need for decision making by an operator arises only rarely. But the entire process is impossible without human involvement.

Analysis of the EW System functioning and non-standard situations that occurred in the past demonstrate that system malfunctioning may arise from multiple causes including:

- Personnel mistakes (human factor)
- Unintended interference from natural phenomena that have not been fully researched and their influence on the system functioning has not been included in algorithms
- Lack of knowledge about BM development and "modus operandi" of different states

In time, as experience is accumulated, the system's tools and algorithms are improved, the volume of input data for processing grows, and the reliability of notifying information increases.

For further BMEW Systems updating and for reducing the risks of decision making on the basis of misrepresented EW information the following proposals should be discussed:

1. Improving the BM launch and space activity notification system. Expanding the number of participant states through the creation of joint/united data exchanges centers.

2. Exchanging of space objects data catalogues on the regular basis (as a future perspective—the exchange in the real time mode).

3. Conducting the joint action on resounded events in space (monitoring and prognosis of dangerous artificial or natural objects landing incidences).

4. Joint training, analysis, and experience exchange for the specialists on near Earth space monitoring.

5. Improving personnel education and training (first, how operators should act in non-standard or crisis situations.)

NC3, BMEWS and Cybersecurity

The idea that a foreign state or non-state actor can intervene in the normal functioning of NC3 systems or BMEW systems is a great concern of each nuclear state. The threat to destroy strategic stability is too important to justify such meddling, let alone attacks. It is impossible to preserve the inviolability of one's own NC3 system unless you recognize that opponents must have the same confidence in their NC3 systems. Perhaps an agreement is needed that commits all states that possess or will possess NC3 and EW systems to not impinge in any way on the NC3 and EW systems of each other. No-one has an interest in starting an accidental nuclear war. Russia and the United States have an old agreement that lays out actions in case of accidental strike. There are also the US-Russia Centers of Risk Reduction. These exchange data, but we need a decision that drives higher levels of commitment to not NC3 systems. It has been proposed to include in Russia's military doctrine that an attack on EW would be interpreted as a sign of impending nuclear attack. Thankfully it was not included in the final version. We do need such an agreement to mutually protect NC3 systems to secure ourselves from an unintended nuclear war.

The Russian NC3 is not prone to a cyber-attack. This is accomplished relatively easily; you have to isolate the system from the Internet. Of course, you can go around that by attacking the electric feed system, but you can apply filters for electric signals and have only a purified signal of 50 Hz 250 V. There are also special security requirements to radio communication channels.

Although the NC3 system can be made secure against cyber-attack, the EW system is quite open to cyber-attack. It is not closed. As to interference from cyber-attacks, etc., this problem has always been present for the input from the radars. But it related not as much to threats but to natural factors like the sun. The sun behaves differently, and our algorithm struggled with that for some time. When the system is tested, it is tested for resistance from all kinds of interference.

In 1990s Russia and the United States had good discussions on EW cooperation including the creation of a Joint Data Exchange Center (JDEC). We were very close to opening the JDEC in Moscow. Unfortunately, the two countries failed to implement this Center. Today, most experts think it was a useful idea. The exchange of EW information is vital to avoid dangerous mistakes in decision making. For example, if an EW system registered a BM launch and even if the warhead landed in protected territory, then a massive retaliatory strike is still not justified. A mistake with the calculated trajectory and the very fact of the launch is possible. Such mistakes still are possible. It could be a terrorist act or a mistake, or it could happen during an exercise, like the August 10, 2019, missile launch in Estonia.[8] Many other situations are possible. Also, it could be a non-nuclear attack, and then the massive response strike cannot be an adequate answer in the legal sense. We face similar problems in space—some satellites are dual-use. In general, the situation with space security is getting close to critical. All these areas require close attention, and it is urgent that cooperation in each dimension begins as soon as possible.

III. ENDNOTES

[8] J. Tanner, "Estonia halts NATO air drills after jet misfires missile," The Associated Press, August 10, 2018, at: https://www.defensenews.com/training-sim/2018/08/10/estonia-halts-nato-air-drills-after-jet-misfires-missile/

IV. TECHNOLOGY FOR GLOBAL SECURITY INVITES YOUR RESPONSE

Technology for Global Security invites your responses to this report. Please send responses to: info@t4gs.org. Responses will be considered for redistribution to the network only if they include the author's name, affiliation, and explicit consent