To: President Barack Obama
FROM: John Smith, Special Asst. to the President and Sr. Director for Russia and Eurasian Affairs
RE: U.S. and/or NATO Response to Cyber Attack on Estonia

Issue. A cyber attack against SCADA systems has caused significant damage to Estonia's utilities with a current attack on the cell phone network. There have been casualties. Options for a U.S. response are needed.

Relevant National Interests.
Vital. Prevent Russia cyber attacks on Estonia public and private sectors; ensure and promote that Estonian sovereignty, physical and within cyberspace, is absolute.
Extremely Important. Affirm NATO deterrence credibility; support that any attack, conventional or cyber falls under the auspices of NATO; Washington Treaty, Article V.
Important. De-escalate rising tensions between the U.S. and Russia; utilize Estonia cyber attack to reach agreement with Russia on similar conflicts including Ukraine.

Analysis. Estonia has been a NATO member state since Mar. 2004. In Sept. 2014 NATO released the Enhanced Cyber Defense Policy; "…that cyber defence is part of NATO's core task of collective defence." In Sept. 2014 President Obama made clear NATO's commitment to Estonia; "We will defend our NATO Allies, and that means every Ally. In this Alliance, there are no old members or new members, no junior partners or senior partners..." In 2008, NATO accepted the use of Estonia's Cyber Range as a core component to establish the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE). NATO also utilizes the Estonian Amari Air Base as a NATO interoperable airfield; conducting NATO Baltic Air Policing patrols beginning April 30, 2014. Beginning in 2015, the aerial assets supporting NATO's American-led Operation Atlantic Resolve (ongoing efforts in response to Russia's actions in Ukraine) are based at Amari.

Vladimir Putin has been the leader of Russia since 1999 serving as either President or Prime Minister. In 1997 NATO and Russia signed the Founding Act on Mutual Relations, Cooperation and Security, stating the "aim of creating in Europe a common space of security and stability, without dividing lines or spheres of influence limiting the sovereignty of any state." Since Putin's rise to leadership he has made it clear that Russia has a legitimate right to a Russian sphere of influence citing historical ties, language and ethnic ties and as a buffer to Western aggression. Russia's desire can be grouped into three categories. First countries where Russia feels it must fully reconsolidate its influence: Belarus, Kazakhstan, Ukraine and Georgia. These countries protect Russia from Asia and Europe and give Russia access to the Black and Caspian seas. Second countries where Putin would like to reconsolidate its influence; Estonia, Latvia, Lithuania, Azerbaijan, Turkmenistan and Uzbekistan. They are geographically too close to the Russian core to allow Western dominance. Last are countries that are not critical to Russia but could easily be controlled (or kept under control) by Russia with ease due to their own inherent vulnerabilities; Moldova, Kyrgyzstan, Tajikistan and Armenia. In addition and related to Russia's desire to rebuild its sphere of influence is Putin's aim at rebuilding nationalistic fervor within Russia through mobilizing Russia's citizenry against a common enemy (the U.S.), and moving from a national feeling of isolationism to that of regional and world super power. It is believed that Russia is currently and will continue to utilize cyber attacks as the tactic of choice to punish countries formerly within the Russian sphere of influence whom seek NATO membership or move too far in their ties to the European Union. Three key drivers must be considered to determine appropriate response to Russian cyber attacks against Estonia:

<u>The cyber attacks against Estonia can clearly be attributed to Russia.</u> Attribution for the current attacks against Estonia point beyond a reasonable doubt to be the work of the Russian government. Under the auspices of the U.S. Cyber Command (USCYBERCOM), the U.S. has a broad program of 'implants' in various countries including Russia. Utilizing these implants, there is clear evidence of the attack massing including seeing the code being written and moving between servers. All evidence points to Russian military cyber units. USCYBERCOM and the National Security Agency have 95% confidence in the attribution.

<u>Russia offensive use of cyber espionage and attacks are increasing and often linked to kinetic military actions.</u> Russia has a history of utilizing cyber attacks both as isolated actions and as part of a broader campaign that

includes traditional kinetic military action. Some of the higher profile Russian sponsored cyber attacks include: 1998-2000 Moonlight Maze, 2007 Estonia, 2008 Georgia, 2009 Lithuania, 2009 U.S. and NATO, 2004-2011 Pawn Storm, 2014 Ukraine, 2014 JPMorgan Chase, 2014 NATO and EU, 2015 Ukraine and 2015 U.S. State Dept. and White House. Cyber attacks by Russia in both Georgia and in the Ukraine were quickly followed by conventional military action. At risk is whether the current Estonian cyber attack is a prelude to kinetic military action by Russia. There has been an increase in conventional military activity in the area around Estonia. Two Estonian intelligence officers working at the CCDCOE had been kidnapped near the Russian border and held hostage by Russian intelligence two weeks ago. Upon release, officers reported that they were forced to divulge classified data. There has been an increase in Russian activity over Baltic airspace. Russian aircraft have been sighted repeatedly in the Baltic Sea area. In Estonia there have been six airspace violations. Russian military planes have been seen flying very close to Latvian and Lithuanian airspace.

Russia has valid concerns on the treatment of ethnic Russians in Estonia. Putin may have some legitimate concerns on the treatment of Estonian's of Russian descent and language. 30 percent of the population in Estonia is ethnic Russian or Russian speaking. Tensions between ethnic nationals and Russian minorities in Estonia, Latvia, and Lithuania have turned into riots; more than 100 people have been killed. The EU has been warning Estonian authorities that they were violating EU rules by putting new pressure on ethnic Russians, including marginalizing some non-citizens and creating obstacles for Russian speakers to attain citizenship. Estonia has prohibited the use of Russian in schools, even in those areas where Russian speakers make up a majority of the students. There have been reports of harassment, of houses being broken into and of intimidation aimed at controlling activist behavior. Politicians on the extreme right in Estonia are threatening deportations, and forcing ethnic Russians to reaffirm their allegiance to Estonia if they wish to stay in the country.

Operational Objectives.

Short-Term

- Stop current Russian cyber attacks against Estonia; eliminate for the short-term Russian desire and/or capability to restart cyber attacks against Estonia
- Proportional, retaliatory response as deterrent

Long-Term

- Establish precedence that cyber attack against a NATO member will be responded in the same way as a kinetic military attack against any NATO country
- Achieve accommodation between Russia and the U.S./NATO regarding western influence in countries formerly within the Russian sphere of influence beginning with Ukraine and Estonia

Strategic Options.

1. **Cyber Protective Response, Select Covert Action and Conventional Military Show of Force**. Remove Russian perception that cyber attacks are low risk for kinetic military retaliation by immediately counseling Estonia to invoke NATO Article V due to Russia's offensive and unlawful breach of Estonia sovereignty and attack on Estonian state and commercial assets. Stop current cyber attack and eliminate operational capabilities of IT assets utilized in the Estonia attack. Through covert action, eliminate select human resources (state and non-state) involved in the attacks. In parallel, NATO to initiate "show of force" in multiple Russian geographic regions including Estonia.
   Pros: A NATO cyber response allow for control, distance and asymmetry. It establishes precedence that cyber attacks fall under NATO Article V. Displaying a conventional "show of force" in multiple Russian geographies without moving to direct kinetic action shows Russia the risk of escalation and will highlight internally Russia's lack of readiness and inability to respond and/or handle a sustained response in multiple theaters simultaneously. Elimination of human resources with direct cyber attack involvement is a proportional response to the fatalities caused and a deterrence to non-state actors pay for service.
   Cons: NATO cyber response risks unveiling U.S. cyber assets to Russia. Conventional show of force establishes precedence for kinetic escalation by U.S. adversaries as well. Covert action poses international

legal challenges. Generational shift in Europe and U.S. coincides with negative attitudinal shift to conventional military action. Public support in NATO countries will be difficult.

2. **Establish European Non-Aligned Organization. Seek UN condemnation of Russia and Reparations.** Utilize a new treaty framework to establish a European non-aligned treaty organization closely aligned to the United Nations. Potential members include Finland, Estonia, Ukraine, Belarus, Kazakhstan, Georgia, Latvia, Lithuania, Azerbaijan, Turkmenistan, Uzbekistan, Moldova, Kyrgyzstan, Tajikistan and Armenia. Seek this non-aligned organization to sign non-aggression pacts both with Russia and NATO. While having no self-defense pact with either Russia or NATO, clearly indicate that any violation of these countries sovereignty's would be considered an act of war with the United Nations fully authorized to respond. Utilize this non-aligned framework to achieve grand solution to current (Estonia and Ukraine) and future East v. West sphere of influence conflicts. In parallel, Estonia to seek UN condemnation of Russia cyber attacks as well as demand for reparations. Consider use of the International Criminal Court as venue.
   Pros: Recognizes that Russia may have legitimate rationale for a Russia sphere of influence and problems with western encroachment into that sphere. Lessens Putin's concern on being a target for regime change. Utilizes existing international legal/international government structures and precedents.
   Cons: Building an international coalition of non-aligned countries is difficult. UN historically racked by inaction with Russia having permanent member status on Security Council and ability to veto action. As with Crimea and Ukraine, permanent harm can be done prior to international action. Undermines NATO credibility in not responding to a direct attack against a member state regardless of invocation of Article V.

3. **Cyber Retaliatory Response Targeting Putin and Elites.** Utilize U.S. offensive cyber capabilities to target Putin and elites personal and commercial assets. Objective is to provide severe economic harm to the personal assets of Putin and elites as a deterrence against future Russia sponsored cyber attacks.
   Pros: Existing U.S. cyber assets (implants) are not revealed. Putin and elites are driven by wealth generation. Linking Russian sponsored cyber attacks to real economic harm to Putin elites will result in pressure on Putin to deter future cyber attacks.
   Cons: Legality of targeting citizens based on the action of the Russian state is not clear. Lack of direct NATO response against a NATO member undermines NATO credibility and lacks establishment of precedence to respond. Attack on Estonia will now become a Russia-U.S. conflict.

Recommendation. Option 1: Cyber Protective Response, Select Covert Action and Conventional Military Show of Force. The attack has caused extensive damage to infrastructure and loss of life. NATO has facilities vital to members in Estonia including CCDCOE and Amir Air Base. NATO's Enhanced Cyber Defense Policy is framework for a response. Cyber is the battlefield of the future and deterrence and precedent must be set now.

Implementation. U.S. Secretary of State to counsel Estonia Ambassador to invoke NATO Article V. NATO Computer Incident Response Capability (NCIRC) team to work immediately to stop current attack. NCIRC to work with USCYBERCOM and NATO CCDCOE to identify all IT assets, physical and human resources, utilized by Russia. This may include state and non-state assets. Under auspices of Supreme Headquarters Allied Power Europe (SHAPE); NCIRC to coordinate offensive response to destroy and/or make inoperable all Russian IT assets involved in the cyber attack. SHAPE to immediately deploy Very High Readiness Joint Task Force (VJTF) to Amir Air Base in Estonia. In parallel, SHAPE to mobilize "show of force" NATO units in Poland, Black Sea/Turkey, Japan (Kuril Islands) and the Artic region/Barents Sea. President Obama through executive order to direct CIA Director of Operations to eliminate Russian state and non-state human resources that were vital to the planning and execution of the attacks.

Strategic Communication. Initiate U.S.-Russia cyber security hotline between the U.S. Cybersecurity Coordinator and the Russian Deputy Secretary of the Security Council. U.S. Secretary of State will provide clear communication regarding a cease and desist of Russia offensive cyber attacks as well as the mobilization of NATO forces as a defensive only measure should Russia escalate this attack in a conventional manner.

Talking Points.

The following talking points are to be utilized in the government's conversations with the New York Times:

- Cyber-attacks are currently being conducted by the Russia against Estonia targeting Estonia's electrical grid, systems related to the oil and gas sector and a current attack is targeting Estonia's cell phone network. Constant reiteration that the facts including attribution by Russia are beyond a reasonable doubt.
- There have been casualties in Estonia due to power outages at health facilities.
- As a NATO member, Estonia is expected to invoke Article 5 of the Washington Treaty; any attack on a NATO member shall be considered an attack against them all. All NATO members are expected to come to the aid of Estonia.
- NATO has implemented the Enhanced Cyber Defense Policy. Rightfully, the policy clearly articulates that in today's technology driven world, an attack in cyber space can and is as damaging as a conventional attack. Cyber or kinetic attacks against NATO members will be dealt with utilizing all the means available to NATO.
- NATO is the organization that will respond to this threat on its member state. The U.S. will provide material support to NATO as necessary.
- Stress that the situation in Estonia is occurring real-time. The media divulging any sensitive, classified information threatens both the defense of Estonia and other NATO members and risks human lives.
- Put forth that the *New York Times* will be given an exclusive interview with President Obama on these events once de-escalation occurs.

Appendix A. Follow-up Questions

1. Perform attribution analysis clearly aligning Russia to the cyber attacks even if conducted by nonstate groups. Solidify and document evidence. Directed to the Director USCYBERCOM.
2. What is the level of cyber response capability within Russia? Update threat and capability assessment of Russia's military cyber unit, attack operations capability and command and control structure. Directed to the Director NATO CDCCOE.
3. What damage has Russia cyber attack inflicted to date? Prepare damage assessment on the Russia cyber attacks including physical and human damage. Directed to U.S. Ambassador to Estonia.
4. What is the legal standing in regards to lethal targeting of non-U.S. citizens abroad in response to their involvement in a cyber attack that has resulted in casualties? Directed to U.S. Attorney General.
5. What options are available to Russia in terms of cyber retaliation? Prepare cyber response options targeting NATO and U.S. private and public assets. Directed to Director, USCYBERCOM.
6. Is there a risk of conventional escalation for a NATO retaliatory cyber-attack? Determine risk of escalation, military and cyberspace, to NATO and U.S. retaliatory measures. Directed to Director, National Security Agency.