Support for Cooperation among Governments to Address Cyber Threats to Nuclear Weapons Systems

We have crossed over to a new nuclear era in which cyber capabilities transform the nuclear risks. A successful cyberattack on nuclear weapons or related systems—including nuclear planning systems, early warning systems, communication systems, and delivery systems, in addition to the nuclear weapons themselves—could have catastrophic consequences.

Cyber threats to nuclear weapons systems increase the risk of use as a result of false warnings or miscalculation, increase the risk of unauthorized use of a nuclear weapon, and could undermine confidence in the nuclear deterrent, affecting strategic stability. The speed, stealth, unpredictability, and challenges of attribution of any particular cyberattack make it exceedingly difficult, if not impossible, to anticipate, deter, and defend against all cyber threats.

All countries with nuclear weapons are vulnerable to cyberattacks, and the potential consequences of any nuclear launch due to miscalculation, unauthorized use, or a failure of nuclear deterrence would have global implications. A cyber intrusion into another nation's nuclear weapons system, even an unintentional intrusion, could prompt a crisis, potentially leading to nuclear use if another nation believed that the intrusion was a precursor to decapitating its nuclear deterrent.

Cyber threats to nuclear weapons systems require a global response. Reducing and managing cyber nuclear risks is an existential common interest for all nations. Governments have a shared responsibility to work together to mitigate these risks. The following actions should be taken in two priority areas to build a better understanding of the global nature of the threat and to develop cooperative approaches to reducing the threat.

- **Initiate bilateral dialogue with Russia.** The United States and Russia should initiate a bilateral dialogue on cyber-nuclear threats (including the threat of third-party interference) to develop mutual understanding on how cyber threats can affect nuclear deterrence and strategic stability—and amplify the potential for miscalculation. Talks should be held with a view toward developing a shared understanding of the potential consequences and identifying practical steps minimizing the risks, through both bilateral and multilateral mechanisms. As an example, countries could seek ways to cooperate internationally to improve early warning systems—including through military-to-military cooperation—to reduce the possibility of a cyber-induced false warning.

- **Increase international cooperation to reduce the cyber threat.** Without multilateral engagement on the cyber threat, unilateral or bilateral efforts to enhance the security of nuclear weapons systems might be considered destabilizing by other nations. Bilateral and multilateral

For the past four years, Des Browne, Wolfgang Ischinger, Igor Ivanov, Sam Nunn, and their respective organizations—the European Leadership Network (ELN), the Munich Security Conference (MSC), the Russian International Affairs Council (RIAC), and the Nuclear Threat Initiative (NTI)—have been working with former and current officials and experts from a group of Euro-Atlantic states and the European Union to test ideas and develop proposals for improving security in areas of existential common interest. The EASLG operates as an independent and informal initiative, with participants who reflect the diversity of the Euro-Atlantic region from the United States, Canada, Russia, and 15 European countries.
dialogue with countries with and without nuclear weapons, with an initial priority on U.S.-Russia and U.S.-China, is crucial.

Bilateral and multilateral dialogues should identify cooperative actions and identify norms and rules of the road—for example, agreement to refrain from using cyberattacks against nuclear weapons systems—as well as confidence building and verification measures that could enhance confidence in future agreements.

The nations in the Euro-Atlantic region are confronting a range of significant issues today. But none should distract from urgently supporting and pursuing practical steps now that can reduce real and potentially catastrophic dangers associated with cyber threats.