DEPARTMENT OF THE ARMY
DEPARTMENT OF SOCIAL SCIENCES
UNITED STATES MILITARY ACADEMY
BLDG 607, LINCOLN HALL
WEST POINT, NY 10996

MADN-SOC 05 November, 2021

MEMORANDUM FOR SCUSA 72

SUBJECT: Russia-America Rivalry and Disruptive Technologies

1. **Issue**: The purpose of this memorandum is to propose policy options for the United States to consider in countering Russian aggression using disruptive technologies.

2. **Strategic Analysis:**
   a. *Russia's capability in the cyberspace*

Russia likely has the capability to launch cyber attacks that target critical infrastructure in the United States, potentially causing immediate harm and long-term disruption with expansive societal and security implications. Actors organizing and perpetrating these attacks include criminal groups operating independent of the Russian government, Russian government actors, and regime-sponsored actors often operating through troll farms.

   b. *Information warfare*

Russian strategy in the operation of information campaigns involves a combination of technical and psychological means to target opponents. This includes sowing political instability in an adversarial state, capitalizing on identified weaknesses, and provoking and deepening sociopolitical divisions and mistrust.The decentralized nature of these attacks combined with the long-term erosion of trust in the social and political domains allows the threat posed by Russia to remain acute and unpredictable. The primary domain of operation for Russia's information campaigns is social media platforms. The use of rapidly maturing advanced technologies such as AI and machine learning is deepening the threat posed by cyberattacks.

   c. *Russia's goal in using disruptive technologies to target the U.S. and U.S. allies.*
      i. Russia perceives its response as defensive, viewing the U.S. and NATO as a threat to its sovereignty. Russia's use of information campaigns is a reflection of its own perception of the U.S. approach to Russia.
      ii. Sowing political instability and tearing at the fabric of American society to induce a state of national vulnerability driven by objectives of territorial expansion and hindering NATO expansion.

3. **Relevant National Interests:**
   a. Protecting U.S. critical infrastructure.
   b. Continuing to improve U.S. offensive cyber capabilities.
   c. Safeguarding privacy and U.S. values while preserving public trust.

MADN-SOC

SUBJECT: Russia-America Rivalry and Disruptive Technologies

d. Guaranteeing the security and protection of our allies from external threats.

4. **Strategic Options and Recommendations:**
   a. Developing Resilience and National Preparedness:
      i. Bolster encryption of key data and secure servers. Training a workforce in data protection and consolidating cyber defense.
      ii. Continue the improvement of U.S. offensive cyber capabilities and posture. Determine what kinds of attacks warrant cyber counterattacks.
      iii. Build public-private partnership that seeks to advance research and technological development in cyber security. Partnering with experts from big tech and social media companies to counter deep fakes and information campaigns. Using advanced technologies, such as AI algorithms, to monitor and detect fake bots and disinformation on public platforms and halt the spread of malign narratives. This should include collaborating on education directed towards the domestic population discussing privacy, safety, and misinformation.
   b. International Cooperation
      i. Building partnerships and coordinating strategies in order to maintain a competitive advantage over Russian aggression in cyberspace.
      ii. Diplomatic engagement
         a. Bilateral engagement to better understand Russia's motivations and come to an informal or formal agreement.
         b. Initiating a multilateral conversation surrounding what constitutes a cyber attack that merits a kinetic response or economic sanctions.
   c. Sanctions policy against infrastructure attacks.
      i. Analysis of current sanctions' effectiveness in achieving U.S. national security objectives, and preparing a plan for sanctions in response to future cyberattacks based off this research
      ii. Maintaining U.S. autonomy in developing a unilateral sanctions regime against Russia if unable to reach a multilateral agreement.

5. The point of contact for this memorandum is CDT Justin Harper at justin.harper@westpoint.edu or 717-422-1430.

Encl

Russia Roundtable
SCUSA 72
United States Military Academy

MADN-SOC

SUBJECT: Russia-America Rivalry and Disruptive Technologies

Encl

References

Critical Infrastructure Sectors, *Presidential Policy Directive 21*, Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/critical-infrastructure-sectors.